浙江省重点专业资助项目
杭州市重点学科资助项目

QUN DE JIEGOU YU DUICHENXING

群的结构与对称性

陈 辉 著



ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

QUN DE JIEGOU YU DUICHENXING



ISBN 978-7-308-06443-9

9 787308 064439 >

定价：37.00元

浙江省重点专业资助项目
杭州市重点学科资助项目

群的结构与对称性

陈 辉 著

浙江大学出版社

图书在版编目（CIP）数据

群的结构与对称性 / 陈辉著. —杭州：浙江大学出版社，2008.12

ISBN 978-7-308-06443-9

Ⅰ.群…　Ⅱ.陈…　Ⅲ.群论　Ⅳ.0152

中国版本图书馆 CIP 数据核字（2008）第 199078 号

群的结构与对称性

陈　辉　著

责任编辑　阮海潮(ruan100@yahoo.cn)

封面设计　刘依群

出版发行　浙江大学出版社

（杭州市天目山路 148 号　邮政编码 310028）

(E-mail：zupress@mail.hz.zj.cn)

（网址：http://www.zjupress.com

http://www.press.zju.edu.cn）

电话：0571—88925592，88273066（传真）

排　　版　杭州中大图文设计有限公司

印　　刷　德清县第二印刷厂

开　　本　787mm×960mm　1/16

印　　张　19

字　　数　430 千

版 印 次　2008 年 12 月第 1 版　2008 年 12 月第 1 次印刷

书　　号　ISBN 978-7-308-06443-9

定　　价　37.00 元

内 容 简 介

群论自19世纪由Galois创立以来，不仅成为近代代数的重要分支，而且其应用范围已深入到科学技术的各个领域. 尤其是自然科学的物理、化学和生物的研究中，群论已成为必不可少的强有力的数学工具. 对称性是自然界最普遍、最重要的特性. 自然界的所有重要的规律均与某种对称性有关，甚至所有自然界中的相互作用，都具有某种特殊的对称性. 虽然对称的概念看来是很明显的，但为了给对称这个概念一个精确的和一般的描述，特别是对称性的量上的计算，却需要利用群论这个工具。本书系统地介绍群的对称性及其应用.

全书共分七章，对称与群初步、群的对称性与群的结构、群表示论基础、代数方程的对称性、物理学中的对称群、分子对称群及Lie群结构的对称性. 其中群与群的表示理论是本书的基础.

本书着眼于方法论的阐述，不仅引入概念，阐述理论，而且附有大量的应用实例，涉及了数学、物理学、化学、材料科学和工程技术各方面，使读者领悟群的对称性的科学含义及广泛应用背景.

前言

群论自19世纪由Galois创立以来，不仅成为近代代数的重要分支，而且其应用范围已深入到科学技术的各个领域．尤其是自然科学的物理、化学和生物的研究中，群论已成为必不可少的强有力的数学工具．

客观世界普遍存在各种各样的对称性，而群论正是描述、反映和研究对称性的数学武器，因此从其诞生至今，就存在一个由纯粹数学领域扩展到其他自然科学领域的必然现象．Galois利用群的对称性证明了五次或五次以上的代数方程不能通过初等代数方法求得方程的精确解．

20世纪，传统群论与现代拓扑学、流形的概念相结合，形成拓扑群的新理论．就在群论不断发展不断现代化的过程中，我们看到许多群论大师，如E. Cantan、H. Weyl、G. Racah、E. P. Wigner等同时又是物理学大师．群论迅速在量子力学、光谱学、角动量理论、原子核谱等物理学领域得到广泛应用．

对称性是自然界最普遍、最重要的特性．《可怕的对称》一书的作者认为，上帝是按照“对称”的美学思想来设计自然的．

近代科学表明，自然界所有重要的规律均与某种对称性有关，甚至所有自然界中的相互作用，都具有某种特殊的对称性——所谓“规范对称性”．实际上，对称性研究的日趋深入，已越来越广泛地应用到物理的各个分支：量子论、高能物理、相对论、原子与分子物理、晶体物理、原子核物理，以及化学(晶体的分类、分子轨道理论、配位场理论等)、生物(DNA的构型对称性等)和工程技术．

虽然对称的概念看来是很明显的，但为了给对称这个概念一个精确的和一般的描述，特别是对称的性质的量上的计算，却需要利用群论这个工具，我们强调“对称即群”的观点．

在 1890 年，Federov 和 Schoen Files 就利用群的对称性系统解决了晶体结构分类问题，证明了具有周期性排列的空间点阵总共有 230 种，使人大开眼界. 1893 年，挪威科学家 Sophus Lie 和 Scheffer 将群论与微分方程结合起来，使有限群的概念扩展到无限群、连续群，导致现代李群的建立.

20 世纪 50 年代末到 60 年代中期，在基本粒子研究中，SU(3)理论、夸克模型等的巨大成功，形成了群论向其他学科"普及"的一次热潮. 时至今日，群对称性的应用领域不仅遍及物理学各个领域，而且扩展到化学、生物、材料科学、流体力学、机械、电工学等等.

群与群的表示理论是本书的基础. 在讨论时我们选择一些较深入的内容，对群论，选择 Sylow 定理、有限交换群的结构定理和 Galois 理论等. 好的数学思想是一定会在不同场合下重复出现的. 使初学者能看到这些重复是有益的. 在本书中分解型结构思想重复出现在有限交换群的结构定理中，Galois 对应思想重复出现在 Galois 理论中.

由于教学的需要，不过于追求数学理论的完备与严格，尽可能从大家较为熟悉的具体事例出发，阐述有关概念；尽可能多地列举应用实例。本书的应用实例，涉及了数学、物理学、化学、材料科学和工程技术各方面。本书着眼于方法论的阐述，希望能起到举一反三的效果，以帮助读者在群论与对称之间架起一座桥梁.

本书的特点是，不仅引入概念，阐述理论内容，还附有大量例题，提出问题，这是很重要的。相对独立地解决这些问题，一定会使读者对基础内容有较深刻的理解. 为便于读者领悟群的对称性的科学含义及广泛应用背景，同时在所有问题中，凡是需要提示的地方，尽量给予详尽提示.

在本书编写过程中，我的学生陈晓玮做了大量工作，给我以很大的帮助，在此表示感谢.

陈　辉

目　录

第1章 对 称

对称性是自然界最普遍、最重要的特性. 自然界所有重要的规律均与某种对称性有关,对称性的研究已越来越广泛地应用到物理学的各个分支:量子论、高能物理、相对论、原子与分子物理、晶体物理、原子核物理以及化学中晶体的分类、生物(DNA 的构型对称性等)和工程技术.

虽然对称的概念看来是很明显的,但为了给对称这个概念一个精确的和一般的描述,特别是对称的性质的量的刻画,却需要利用群论这个工具. 我们探讨平面上有限图形的对称,人们都会说圆比正方形更对称些,正六边形比正三角形更显得对称一些. 如果问正方形和正六边形谁更对称一些,该怎么回答呢? 无论是单个图形还是带型、壁纸型对称图案都可用群来准确描述. 本章将讨论对称与群,并将强调群概念产生的背景,群是对称概念的数学描述,研究群就是为了研究复杂的对称. 希望读者能对"对称即群"有一个初步的理解.

§1.1 图形的对称

什么是对称性? 按照英国《韦氏国际辞典》中的定义:"对称性乃是分界线或中央平面两侧各部分在大小、形状和相对位置的对应性."这里追溯到最直观、最早为人们熟知的所谓几何对称性. 空间一点 A 叫做点 B 关于平面 M 的对称点,如果这平面垂直地交线段 AB 于其中点,通常说 B 点是点 A 关于平面 M 的反射象. 说一个几何体关于平面是对称的,如果这个平面把几何体劈成两部分,其中任一部分都是另一部分关于所给镜面映象,此时这个平面被称为物体的对称平面.

对称性是"适当或协调的比例,以及由这种和谐产生的形式美". 这里依然谈的是空间的几何对称性,尽管涉及对称性的美学属性,实际上,对称性的现代科学概念极难定义,几乎成为规律和和谐的同义语,它与所谓不变性、守恒律往往结下不解之缘. 对称性分两大类:与时间、空间有关的,称为几何对称性;否则称为内禀对称性.

定义 1.1.1 具有某种对称性的图形,就是经过某些刚体运动后仍能回到自身的图形.

也许这就是圆比正方形更对称的解释.用使图形回到自身的所有运动来刻画这一图形的对称应该是自然的,也符合我们对对称的直观感觉.例如,圆经过绕圆心的任意旋转以及以任何过圆心的直线为轴的反射都回到自身,正方形绕其中心旋转 $\pi/2,\pi,3\pi/2,2\pi$ 或以其对角线和对边中点连线的反射才能回到自身,而梯形就更差了,它只有绕其中心旋转 $2k\pi$ 才能回到自身,因此所谓对称是与变换联系在一起的.

例 1.1.1　两端无限延伸的直线,上面有等距离 d 的刻度(如图 1.1).

直线向左或向右平行移动 d 的整数倍,仍然与原直线重合(不变性),或相对任一刻度点或两相邻刻度点的中点进行反射,亦与原直线重合,故该直线具有等距离 d 的整数倍的平移对称性和相对刻度点(中点)的反射不变性.

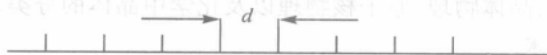


图 1.1　有等距离刻度的无限直线

例 1.1.2　等边三角形和直圆柱体(如图 1.2).

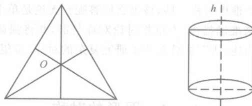


图 1.2

能使图形复原的变化,称为该图形的对称变换或对称操作.等边三角形的全部对称操作是:绕中心 O 转动角 0°(不动)、$2\pi/3$、$4\pi/3$ 、(ρ_0,ρ_1,ρ_2);关于每个角平分线的反射(常记为 m_a,m_b,m_c).

直圆柱体的全部对称操作是:绕圆柱轴线 h 转动任意角度(有无穷多个操作);上述转动后,再相对于圆柱的中心 O 反演;相对于过轴线 h 的任一平面的反射;绕过中心 O 且垂直于轴线的任一直线转动角 π.

定义 1.1.2　平面中一个图形 S 的对称变换是指平面内具有性质 $T(S)=S$ 的保距变换 T.(后面还要详细讨论)

平面中一个图形的对称变换实际上即指旋转、平移、反射.上面的三种对称变换的任意复合都正好还是这三种的某一种.复合为群的定义中的二元运算作铺垫.一个平面图形的所有对称变换的复合还是这个图形的对称变换,此为群论定义中的封闭性作铺

垫.旋转为 0°的特殊对称变换,实际对应着群定义中的单位元.而对称中的反对称正是群定义中的逆元.

定义 1.1.3 一个平面图形的对称变换群是指图形的所有对称变换的集合.

此定义不是抽象群的描述,但作为群论学习的前奏,非常自然,且与后续的“变换群”相呼应.

例 1.1.3 如图 1.3 所示的三角形,具有 0°、120°、240°的三个旋转,因而组成了一个三阶对称变换群,实际上是一个循环群 C_3.又如上图所示的太阳八角星,具有八个旋转和八个反射,组成了二面体群 D_{16}.



图 1.3

【问题】 将图 1.3 中的三角形内的字符 a 移走,还是三阶对称变换群吗?将图 1.3 中的八个角内各插入一个字符“a”,情况会怎样呢?

定义 1.1.4 带型图案是指平移对称向量总具有形式 nV 的图案,其中 n 是整数,V 是固定向量.



图 1.4

【思考】分析图 1.4 中的带型对称图案.

§1.2 对称变换

定义 1.2.1 一个 A 到 A 的映射叫做 A 的一个变换.

一个 A 到 A 的满射、单射或 A 与 A 间的一一映射叫做 A 的一个满射变换、单射变换或一一变换.

变换,尤其是一一变换,也是近世代数里极重要的概念.

例 1.2.1 $A=\mathbf{Z}, f: x\longmapsto \frac{x}{2}$, x 是偶数; $x\longmapsto \frac{x+1}{2}$, x 是奇数,是 A 的一个满射变换.

例 1.2.2　$A=\mathbf{R}, f: x\longmapsto e^x$ 是 A 的一个单射变换.

例 1.2.3　$A=\{1,2,3\}, B=\{a,b,c\}$

$$f_1: 1\longmapsto a,\quad 2\longmapsto b,\quad 3\longmapsto c;$$

$$f_2: 1\longmapsto b,\quad 2\longmapsto c,\quad 3\longmapsto a.$$

都是 A 的一一变换.

但现在为便利起见,对于变换这种特殊的映射要用一种特殊的符号来说明,我们用符号

$$\tau: a\rightarrow a^{\tau}=\tau(a)$$

当然不是 a 的 τ 次方的意思,因为 τ 是一个变换,a 的 τ 次方根本没有什么意义,这只是一个符号,正如我们对于特殊的映射:代数运算以及关系都用特殊的符号一样.一个集合 A 在一般情形之下当然可以有若干个不同的变换,我们再举一个简单的例子.

例 1.2.4　$A=\{1,2\}$.

$$\tau_1: 1\rightarrow 1, 2\rightarrow 1$$

$$\tau_2: 1\rightarrow 2, 2\rightarrow 2$$

$$\tau_3: 1\rightarrow 1, 2\rightarrow 2$$

$$\tau_4: 1\rightarrow 2, 2\rightarrow 1$$

是 A 的所有的变换,其中 τ_3,τ_4 是一一变换.

现在我们把给定的一个集合 A 的全体变换放在一起,作成一个集合

$$S=\{\tau,\lambda,\mu,\cdots\}$$

我们要想法规定一个 S 的代数运算,这个代数运算我们把它叫做乘法.我们看 S 的两个元 τ 和 λ,

$$\tau: a\rightarrow a^{\tau}, \lambda: a\rightarrow a^{\lambda}$$

那么 $a\rightarrow(a^{\tau})^{\lambda}$,显然也是 A 的一个变换,因为给了 A 的任意元 a,我们可以得出一个唯一的 $(a^{\tau})^{\lambda}$ 来.现在我们规定,就把这个变换叫做 τ 与 λ 的乘积.

$$\tau\lambda: a\rightarrow(a^{\tau})^{\lambda}=a^{\tau\lambda}$$

这样,这个乘法是一个 S 的代数运算.我们举一个例子.

例 1.2.5　我们在例 1.2.4 里取几个变换来算一算它们的乘积.

$\tau_1\tau_2: 1\rightarrow 2, 2\rightarrow 2$,所以 $\tau_1\tau_2=\tau_2$;

$\tau_2\tau_1: 1\rightarrow 1, 2\rightarrow 1$,所以 $\tau_2\tau_1=\tau_1$.

我们说,如上规定的乘法适合结合律:$\tau(\lambda\mu)=(\tau\lambda)\mu$.

因为 $\tau(\lambda\mu): a\rightarrow(a^{\tau})^{\lambda\mu}=((a^{\tau})^{\lambda})^{\mu}$, $(\tau\lambda)\mu: a\rightarrow(a^{\tau\lambda})^{\mu}=((a^{\tau})^{\lambda})^{\mu}$,

对于这个乘法来说,S 有一个单位元,就是 A 的恒等变换 $\varepsilon: a\rightarrow a$,

因为 $\varepsilon\tau: a\rightarrow(a^{\varepsilon})^{\tau}=a^{\tau}$, $\tau\varepsilon: a\rightarrow(a^{\tau})^{\varepsilon}=a^{\tau}$, $\varepsilon\tau=\tau$, $\tau\varepsilon=\tau$.

这样，S 对于这个乘法来说已经满足：乘法适合结合律，有单位元. 下边我们考虑 S 中的元是否都有逆元.

上面例 1.2.4 中的 τ_1，用一个任意的 τ 从左边来乘 τ_1，得到 $\tau\tau_1：1\to 1, 2\to 1$，这就是说，不管 τ 是 A 的哪一个变换，$\tau\tau_1\neq\varepsilon$，也就是说 τ_1 没有逆元.

我们取 S 中的所有一一变换，记为 G，则 G 中每一个元都有逆元.

定理 1.2.1 一个集合 A 的所有一一变换构成的集合，对于上面规定的乘法，乘法适合结合律，有单位元，并且每一个元都有逆元.

证明 首先说明 G 对乘法是封闭的.

i. 假如 τ,λ 是一一变换，那么 $\tau\lambda$ 也是一一变换.

因为在 A 里取一个任意元 a，由于 λ 是一一变换，在 A 里存在 b 有以下性质，

$\lambda: b\to a=b^{\lambda}$,

由于 τ 是一一变换，在 A 里有 c 有以下性质，

$\tau: c\to b=c^{\tau}$,

这样，$\tau\lambda: c\to (c^{\tau})^{\lambda}=b^{\lambda}=a$,

所以 $\tau\lambda$ 是 A 到 A 的满射，假如 $a\neq b$，那么 $a^{\tau}\neq b^{\tau}$，$(a^{\tau})^{\lambda}\neq(b^{\tau})^{\lambda}$，$a^{\tau\lambda}\neq b^{\tau\lambda}$，所以 $\tau\lambda$ 是一一变换；

ii. 结合律对于一般的变换都对，所以对于一一变换也对；

iii. ε 是一一变换，是单位元；

iv. 设 τ 是一个任意的一一变换，那么存在一个一一变换 λ，有以下性质，

$\lambda: a\to a^{\lambda}$，假如 $(a^{\lambda})^{\tau}=a$,

所以 $\lambda\tau: a\to (a^{\lambda})^{\tau}=a$，即 $\lambda\tau=\varepsilon$，称 λ 为 τ 的逆变换，记为 $\lambda=\tau^{-1}$.

例 1.2.6 设 $A=\mathbf{R}$，求证：$G=\{f_{a,b}\mid f_{a,b}: x\mapsto ax+b, a,b\in\mathbf{Q}$，且 $a\neq 0\}$ 对于变换的乘法满足上面四个条件.

证明 i. 设 $f_{a,b},f_{c,d}\in G$，那么 $f_{a,b}\cdot f_{c,d}\in G$.

因为在 A 里取一个任意元 x，由于 λ 是一一变换，在 A 里存在 b 有以下性质，

$f_{c,d}: x\to cx+d^{\lambda}$,

$f_{a,b}: cx+d\to a(cx+d)+b=acx+(ad+b)$,

这样，

$$f_{a,b}\cdot f_{c,d}: x\to acx+(ad+b),$$

即

$$f_{a,b}\cdot f_{c,d}=f_{ac,(ad+b)}.$$

ii. 结合律对于一般的变换都成立；

iii. 显然 $\varepsilon: x\to x$ 是单位元；

iv. 任意 $f_{a,b}\in G$，设 $f_{c,d}$ 是其逆变换，

则 $\varepsilon=f_{a,b}\cdot f_{c,d}=f_{ac,(ad+b)}=:x\rightarrow acx+(ad+b)$，那么 $ac=1, ad+b=0$，

解之得，$c=1/a, d=-b/a$，所以 $f_{1/a,-b/a}$ 是 $f_{a,b}$ 的逆元.

定义 1.2.2　一个有限集合的一个一一变换叫做一个置换.

例 1.2.7　$A=\{1,2,3\}$，

$f_1: 1\mapsto 1,\quad 2\mapsto 2,\quad 3\mapsto 3;$

$f_2: 1\mapsto 1,\quad 2\mapsto 3,\quad 3\mapsto 2;$

$f_3: 1\mapsto 2,\quad 2\mapsto 1,\quad 3\mapsto 3;$

$f_4: 1\mapsto 2,\quad 2\mapsto 3,\quad 3\mapsto 1;$

$f_5: 1\mapsto 3,\quad 2\mapsto 2,\quad 3\mapsto 1;$

$f_6: 1\mapsto 3,\quad 2\mapsto 1,\quad 3\mapsto 2.$

也记为：$f_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}; f_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}; f_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix};$

$f_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}; f_5=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}; f_6=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix};$

以上的表示方法不仅是一个符号.因为不管上一行的 n 个数字的次序如何，这样一个符号都能具体地告诉我们，它所表示的置换 π 是怎样的一个置换；换一句话说，它能告诉我们，经过这个 π，某一个元 a 的象是什么，我们只须在上一行把 i 找到，然后看一看底下是一个什么数字就行了，因此，利用这种符号可以直接来计算两个置换的乘积.我们举一个例.

定理 1.2.2　含 n 个元素的任意集合共有 $n!$ 个一一变换.

证明　设 $M=\{1,2\cdots n\}$，则对 M 的每个一一变换 f，都能确定元素 $1,2\cdots n$ 的一个全排列 $f(1),f(2)\cdots f(n)$.反之，元素 $1,2\cdots n$ 的任意一个全排列都确定 M 的一个双射变换，而且不同的排列确定不同的双射变换，因此，这 n 个元素有多少个全排列，M 就有多少个双射变换.由于 n 个元素共有 $n!$ 个全排列，故 M 共有 $n!$ 个双射变换.

定义 1.2.3　一个 n 元置换把 a_1 变成 a_2，a_2 变成 $a_3\cdots a_{k-1}$ 变成 a_k，a_k 变成 a_1，而使其余元素保持不变的置换，叫做一个 **k-循环置换**.

这样一个置换我们用符号 $(i_1,i_2\cdots i_k)$ 来表示.

例如：$\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}=(1\ 2\ 4)$；$\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}=(1)$

一个任意的置换当然不一定是一个循环置换.

例如：$\begin{pmatrix}1&2&3&4&5\\1&3&2&5&4\end{pmatrix}$ 就不是一个 4-循环置换，实际上它是两个循环置换的乘

积：

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 2 & 5 & 4\end{pmatrix}=(2\ 3)(4\ 5).$$

一般来说，我们有

定理 1.2.3 每一个 n 元置换 π 都可以写成若干个没有共同数字的（不相连的）循环置换的乘积.

证明 我们用归纳法. 当 π 不使任何元变动的时候，就是当 π 是恒等置换的时候，定理是对的.

假定对于最多变动 $r-1(r\leqslant n)$ 个元的 π 定理是对的. 现在我们看一个变动 r 个元的 π，我们任意取一个被 π 变动的元 i_1，从 i_1 出发我们找 i_1 的象 i_2，i_2 的象 i_3，… 这样找下去，直到我们第一次找到一个 i_k 为止，这个 i_k 的象不再是一个新的元，而是我们已经得到过的一个元：$(i_k)^\pi=i_j$，$j\leqslant k$，因为我们一共只有 n 个元，这样的 i_k 是一定存在的. 我们说，$(i_k)^\pi=i_1$.

因为 $i_j(2\leqslant j\leqslant k)$ 已经是 i_{j-1} 的象，所以不能再是 i_k 的象，这样，我们得到

$$i_1\to i_2\to i_3\cdots\to i_k\to i_1$$

因为 π 只使 r 个元变动，$k\leqslant r$. 假如 $k=r$，π 本身已经是一个循环置换，我们用不着再证明什么；假如 $k<r$，有

$$\begin{aligned}\pi &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n\\ i_2 & i_3 & \cdots & i_1 & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n\end{pmatrix}\\ &= \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n\\ i_2 & i_3 & \cdots & i_1 & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n\end{pmatrix}\cdot\\ &\quad\ \begin{pmatrix} i_1 & i_2 & \cdots & i_k & i_{k+1} & \cdots & i_r & i_{r+1} & \cdots & i_n\\ i_1 & i_2 & \cdots & i_k & i'_{k+1} & \cdots & i'_r & i_{r+1} & \cdots & i_n\end{pmatrix}\\ &= (i_1\, i_2\cdots\, i_k)\cdot\pi_1,\cdots\end{aligned}$$

但 π_1 只使得 $r-k<r$ 个元变动，照归纳法的假定，可以写成不相连的循环置换的乘积：$\pi_1=\eta_1\eta_2\cdots\eta_m$，在这些 η 里，$i_1,i_2\cdots\, i_k$ 不会出现，不然的话，

$$\eta_t=(\cdots\, i_p,i_q\cdots)\qquad p\leqslant k$$

那么 i_p 同 i_q 不会再在其余的 η 中出现，π_1 也必使 $i_p\to i_q$，但我们知道，π_1 使得 i_p 不动，这是一个矛盾，这样，π 是不相连循环置换的乘积.

$$\pi=(i_1\, i_2\cdots\, i_k)\eta_1\eta_2\cdots\,\eta_m\, i_q$$

例如：S_4 的全体元素可以表示成：

(1)

(1 2)，(1 3)，(1 4)，(2 3)，(2 4)，(3 4)

(1 2 3),(1 2 4),(1 3 2),(1 3 4),(1 4 2),(1 4 3),(2 3 4),(2 4 3)

(1 2 3 4),(1 2 4 3),(1 3 2 4),(1 3 4 2),(1 4 2 3),(1 4 3 2),

(1 2)(3 4),(1 3)(2 3),(1 4)(2 3).

用循环置换来表示置换的方法比第一种方法简单,并且能告诉我们每一个置换的特性. 比方说,在例 1.2.7 里我们可以由这种表示方法看出,S_4 的元可以分成五类,每一类的元的性质一定相同,所以计算置换群用第二种方法的时候比较多. 当然在特殊情形之下,也有用第一种方法比较方便的时候.

定义 1.2.4 一个具有某些关系的集合到自身的保持这些关系不变的变换,称为对称变换.

一个具有某些关系的集合的对称性好是指集合上具有比较多的对称变换.

两个对称变换的合成是对该集合连续做两次对称变换的变换,一个集合上的对称变换的集合 G 对对称变换的合成来说具有下列性质:

i. 对称变换的合成还是对称变换;

ii. 对称变换的合成满足结合律;

iii. 恒等变换与任何对称变换的合成等于该对称变换;

iv. 每一个对称变换都有逆变换.

某特定的这样的集合 G 中元素(变换)的个数、元素之间的关系以及所有这样的集合 G 的分类问题是对称问题的重要内容."群"作为代数中最基本的概念之一是比较抽象的,但它只是现实中所谓对称概念的抽象描述.

问题 1.2

1. 找出所有 S_3 的不能和(1 2 3)交换的元.
2. 把 S_3 的所有的元写成不相连的循环置换的乘积.
3. 证明:两个不相连循环置换可以交换.
4. 证明:$(i_1\, i_2 \cdots i_k)^{-1}=(i_k\quad i_{k-1}\cdots i_1)$.
5. 证明:$(i_1\, i_2 \cdots i_k)$的阶数是 k.
6. 证明:S_n 的每一个元都可以写成对换(1 2),(1 3),(1 4),…(1 n)的乘积.

§1.3 平面运动

定义 1.3.1 平面的**保距变换**是保持平面上任何两点的距离都不变的变换(是一种对称变换).

平面的保距变换的集合 $M(\mathbf{R}^2)$对于保距变换的合成构成群,$(M(\mathbf{R}^2),\cdot)$称为平

面的保距变换群.

在这里我们首先回忆一下平面及其运动的概念.

用朴素平面几何的说法,可把平面想象为可向各方无限延伸的黑板面,我们还有平面上的点及两点距离的概念.用解析几何的说法,平面就是集合 $\mathbf{R}^2$(用线性代数的语言,平面也就是二维欧氏空间),今后我们把关于平面 P 的这两种刻画——几何直观的刻画和代数语言的刻画——等同起来.

定义 1.3.2(几何的定义) 平面 P 的一个运动是指平面 P 的一个保距变换.亦即若 f 是平面 P(点集)的一个变换,且对 P 上任意 A、B,$f(A)$和 $f(B)$的距离等于 A 和 B 的距离,则称 f 为平面 P 的一个运动.平面运动是 P 的一一对应.

定理 1.3.1(代数形式) 平面 $\mathbf{R}^2$ 的一个运动,是且仅是 $\mathbf{R}^2$ 中具有下面形式的变换:

$$f:\mathbf{R}^2\to\mathbf{R}^2$$
$$(x,y)\longmapsto(x',y')$$

且 $(x',y')'=O(x,y)'+(a,b)'$,其中 O 是 2 阶正交阵,$A=(a,b)'$是一个取定的列向量.

定理 1.3.1′(几何形式) 平面的运动有且只有下列三种:

a) 沿任一给定向量的平移;

b) 以任意点为中心的旋转;

c) 绕某一直线作反射后再沿该直线上的一个向量作一平移.

我们还知道,在定理 1.4.1 中当 $A=(0,0)'$,而 $\det O=1$ 时,运动 f 就是绕原点的旋转,而当 $A=(0,0)'$,而 $\det O=-1$ 时,f 就起以某一过原点的直线为轴的反射;而 $O=\boldsymbol{I}$ 单位矩阵时,f 就是沿向量 $A=(a,b)'$的平移.

非常重要的是,两个变换是可以相乘的,这就是 M 是一个非空集合,f 和 g 是 M 的两个变换.规定 M 到自身的映射 $h(x)=f(g(x))$(对$\forall\ x\in M$),则易知 h 是 M 的变换.我们定义 h 是变换 f 和变换 g 的乘积,记作 $h=f\cdot g$.注意到 M 的两个一一变换的乘积仍是一个一一变换.

我们把 M 的一一变换全体记作 $T(M)$,并把映射

$$T(M)\times T(M)\to T(M)$$
$$(f,g)\longmapsto f\cdot g,$$ 称为 $T(M)$的一个乘法.

定义 1.3.3 M 是一个非空集合,$T(M)$是 M 的所有一一变换的全体.我们把 $T(M)$及变换的乘法放在一起来考察,记作$(T(M),\cdot)$(这里 · 表示变换的乘法),并称之为 M 的变换群.

定理 1.3.2 变换群$(T(M),\cdot)$具有下列性质:

i. 封闭性，$\forall f,g\in T(M)$，有 $f\cdot g\in T(M)$；

ii. 结合律，$\forall f,g,h\in T(M)$，$(f\cdot g)\cdot h=f\cdot(g\cdot h)$；

iii. 单位元，存在 $\boldsymbol{I}\in T(M)$，使得对于 $\forall f\in T(M)$，有 $\boldsymbol{I}\cdot f=f\cdot\boldsymbol{I}$；

iv. 逆元，对于 $\forall f\in T(M)$，存在 $f^{-1}\in T(M)$，使得 $f\cdot f^{-1}=f^{-1}\cdot f=\boldsymbol{I}$.

现在我们从一般集 M 及其一一变换回到平面 $\mathbf{R}^2$ 及其运动上来. 用 $M(\mathbf{R}^2)$ 表示平面 $\mathbf{R}^2$ 的所有运动，运动只不过是特殊（等距）的一一变换，即有 $M(\mathbf{R}^2)\subseteq(T(\mathbf{R}^2))$，后者是 $\mathbf{R}^2$ 的所有一一变换的全体.

很容易证明：平面的两个运动（保距变换）的乘积仍是一个运动，一个运动的逆变换仍是一个运动. 当然恒等变换是一个保距变换.

这样我们就得到

定理 1.3.3　$M(\mathbf{R}^2)$ 对于变换的乘法具有下列性质：

i. 封闭性，$\forall f,g\in T(\mathbf{R}^2)$，有 $f\cdot g\in T(\mathbf{R}^2)$；

ii. 结合律，$\forall f,g,h\in T(\mathbf{R}^2)$，$(f\cdot g)\cdot h=f\cdot(g\cdot h)$；

ii. 单位元，存在 $\boldsymbol{I}\in T(\mathbf{R}^2)$，使得对于 $\forall f\in T(\mathbf{R}^2)$，有 $\boldsymbol{I}\cdot f=f\cdot I$；

iv. 逆元，对于 $\forall f\in T(\mathbf{R}^2)$，存在 $f^{-1}\in T(\mathbf{R}^2)$，使得 $f\cdot f^{-1}=f^{-1}\cdot f=\boldsymbol{I}$.

很自然地，我们该有下面的

定义 1.3.4　称 $M(\mathbf{R}^2)$ 为平面 $\mathbf{R}^2$ 的运动群. 这里 · 表示运动的乘法（也就是变换的合成，后面的乘法符号省略）.

现在考察使平面图形 K 仍回到自身的平面运动的全体，把它记作 $S(K)$.

平面图形 K 也就是平面 $\mathbf{R}^2$ 上的点集，即 $K\subseteq\mathbf{R}^2$，且 K 中任意两点间有距离；而使 K 保持不变的运动也就是使 $f(K)=K$ 的运动 f（这里 $f(K)=\{f(x)\mid x\in K\}$.

定义 1.3.5　我们把 $S(K)$ 称作平面图形 K 的对称.

这样，我们就把图形 K 的直观对称的概念用精确的数学语言——集合 $S(K)$ 来刻画：K 的对称就是集合 $S(K)$. 我们当然无法"证明"，这个 $S(K)$ 就是你心目中的对称，$S(K)$ 只是我们心目中直观对称概念的一个数学模型. 然而从实践上来看，这个数学模型是可以接受的，是好的. 我们容易证明下面

定理 1.3.4　$(S(K),\cdot)$ 满足上面命题中的 i. ～iv. 这四个条件.

定义 1.3.6　我们称 $(S(K),\cdot)$ 为平面图形 K 的对称变换群.

例 1.3.1　使平面上的正方形仍回到自身的平面运动的全体刻画了正方形对称性的程度. 但若正方形和自己重合，则两对角线的交点也必然要和自己重合. 因此，所求运动使正方形中心不动，因而或是绕中心的旋转，或者关于通过中心的直线的映射. 由图 1.5 容易看到，正方形 $ABCD$ 是关于绕其中心作 $90°$ 倍数角的旋转对称的，对于关于对角线 AC，BD 和直线 KL，MN 的映射，它也是对称的. 这八个运动也就刻画着正方形的

对称.

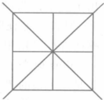


图 1.5

长方形的对称的集合由绕中心作 180°的旋转和关于对边中点连线的映射组成，而平行四边形对称的集合则仅由绕中心作 180°倍数角的旋转组成，即由关于中心的映射和恒等变换组成(图 1.6).

正方形的对称变换群(图 1.6)是由下列平面运动组成：恒等运动，绕其中心转 $0,\pi/2,\pi,3\pi/2$ 的旋转，以及关于它的两条对角线、两条对边中点连线所作的反射，一共 8 个运动.



图 1.6

很容易验证这 8 个运动，使正方形仍回到自身上去. 另一方面利用 Chasles 定理可得其他的平面运动都不使该正方形回到自身.

由于图形的对称性可由对称变换群这一代数对象来刻画，下一步我们就可用代数方法来研究图形的对称，这有点儿像笛卡尔坐标系把几何图形和方程式 C 联系起来后，可用代数方法研究几何一样，不同的是在解析几何中我们用的是多项式，而这一次是用“群”了.

问题 1.3

1. 设 f 是平面 $\mathbf{R}^2$ 的一个运动，其代数形式为：

$$f:\mathbf{R}^2\to\mathbf{R}^2 \qquad (x,y)\longmapsto(x',y')$$

满足 $(x',y')'=O(x,y)'+(a,b)'$，其中 O 是 2 阶正交阵，证明：如果 $\det O=-1$，那么存在一条直线 l，使得运动 f 是关于直线 l 的对称变换，即对于任意的 $A=(x,y)\in\mathbf{R}^2$，有 $(x',y')\in\mathbf{R}^2$ 是 A 的关于直线 l 的对称点，从而 f 是绕 l 的反射.

2. 设 M 是一个非空集合，证明：变换群 $T(M)$ 满足结合律.

3. 设 K 是正六边形，写出 K 的对称变换群 $S(K)$.

§1.4 对称变换群

群论的产生最早源于对代数方程求根的研究，一元二次方程的代数解法早在公前 2000 年就为古巴比伦人所知道，一般三次和四次方程的求根公式也在 16 世纪由意大利数学家费罗(S. Ferro，1465—1526)、塔塔利亚(Fontana，1499?—1557)、卡尔丹(G. Cardano，1501—1576)和费拉里(L. Ferrari)先后获得. 在随后的近 300 年间，数学家们希望能找到五次或更高次方程的求根公式，但都徒劳无功. 直到 1770 年，拉格朗日才第一个宣布“不可能用根式解四次以上方程”，但他却不能证明这个论断. 1799 年，鲁菲尼

给出了一个证明，但他的证明是不完整的. 1824 年，年轻的 Abel 给出了第一个严格的证明. Abel 虽然证明了“五次及五次以上的一般方程没有根式解”，但他并没有解决究竟哪些方程可用根式求解. 这一问题最终被天才的 Galois(1811—1832)所解决(1831 年). Galois 研究了多项式 $f(x)$的根的置换所构成的集合，由于任何两个根的置换的乘积仍是一个根的置换，所以多项式的根的置换全体关于置换的乘积构成一个代数系统，Galois 把这个代数系统叫做群. Galois 发现，方程的可解性与多项式 $f(x)$的根的某些特殊的置换所构成的群之间存在着密切的联系. 他仔细地研究了这个群的结构，并引入了众多概念，如子群、指数、正规子群、可解群等(这些都是群论中的经典内容)，并最终揭示了这种联系. 他证明，一个方程可用根式解的充分必要条件是它的 Galois 群是可解群.

Galois 是把群这个概念引入数学的第一人. 当然，Galois 所说的群不过是一个具体的群——置换群. 置换群不仅在 Galois 的理论中扮演着重要的角色，而且也是研究几何体的对称、晶体的结构等所不可缺少的工具. 今天，置换群已不仅在数学上，而且在物理、化学、计算机科学上都有着广泛的应用，甚至在美学和艺术领域，也日益发挥着它巨大的作用.

自然界中充满了对称的现象. 而现实世界的这种对称现象总是以某种方式与置换群相联系. 艺术家和科学家发现，可以用置换和置换群来很好地刻画他们在艺术创作和科学研究中所遇到的种种对称现象. 艺术家们使用对称与置换来帮助他们设计与构造美妙的图案，物理学家们使用对称与置换来确定晶体的种类，化学家们使用对称与置换去研究分子内部的结构.

也许，一个最具说服力的例子是，1962 年，物理学家格尔曼(M. Gell-Mann，1929—，获 1969 年诺贝尔物理学奖)和尼曼(Y. Ne'eman)应用群的理论预言，存在着一种被称为 Ω-负粒子的新粒子，两年之后这个预言在实验室里被证实，这充分显示了理论对于实践的指导意义.

这一节中，我们将通过例子来说明置换在研究对称变换中的应用.

定义 1.4.1 使图形不变形地变到与自身重合的变换称为这个图形的对称变换. 一个图形的一切对称变换关于变换的乘法构成群，这个群称为这个图形的对称变换群.

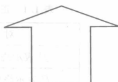
一个图形的对称变换群常可以用一个置换群来表示，它能很好地反映图形的对称性质，是研究图形的对称性质的有力工具.

例 1.4.1 仅由单位(恒等)变换所组成的对称群 K_1. 这是任意非对称形(图 1.7)的对称群.

例 1.4.2 由单位变换及关于某一直线的翻褶组成的对称群(图 1.8).

例 1.4.3 求正方形的对称变换群.


图 1.7


图 1.8

由图 1.8 不难看出,正方形的对称变换只有两种:

1)分别绕中心点 O 按逆时针方向旋转 90°、180°、270°、360°的旋转;

2)关于直线 L_1、L_2、L_3、L_4 的镜面反射.

为了用置换来表示正方形的对称变换,我们用数字 1、2、3、4 来代表正方形的四个顶点(图 1.9),显然,正方形的每一个对称变换都导致了这四个顶点的一个置换.如果对称变换将顶点 i 变为顶点 k_i,那么我们用置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ k_1 & k_2 & k_3 & k_4 \end{pmatrix}$$

来表示这个对称变换.

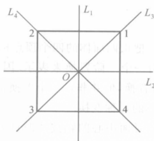


图 1.9

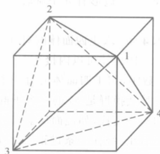


图 1.10

易知,由正方形的每一个对称变换,都可唯一地确定一个 4 阶置换,且不同的对称变换对应于不同的置换.所以正方形的每一个对称变换,都可用唯一的一个四阶置换来表示.表 1.1 列出了正方形的对称变换及其相应的置换表示.

表 1.1　正方形的对称变换及其相应的置换表示

对称变换	置换表示
f^1 表示绕中心旋转 90°	(1 2 3 4)
f^2 表示绕中心旋转 180°	(1 3)(2 4)
f^3 表示绕中心旋转 270°	(1 4 3 2)
f^4 表示绕中心旋转 360°	(1)
g 表示关于直线 L_1 的反射	(1 2)(3 4)
g_2 表示关于直线 L_2 的反射	(1 4)(2 3)
g_3 表示关于直线 L_3 的反射	(2 4)
g_4 表示关于直线 L_4 的反射	(1 3)

由上表可知，两个对称变换的乘积对应于相应的置换的乘积. 所以正方形的对称变换群是 S_4 的一个子群，记作 D_4.

一般地，正 n 边形($n\geqslant 3$)的对称变换群是 S_n 的一个子群，记作 D_n，称为二面体群. 易知，正 n 边形有 n 个旋转(包括恒等变换)和 n 个反射，所以二面体群的阶数是 $2n$.

例 1.4.4　求正四面体的对称变换群.

一个正四面体可以内接于一个正方体(图 1.10). 把正四面体的四个顶点标上 1、2、3、4 四个数字，则正四面体的每一个对称变换都可用一个 4 阶置换来表示. 因此，正四面体的对称变换群是 S_4 的一个子群，共有 24 个 4 阶置换，但并非每一个置换都表示正四面体的对称变换，如镜面反射(1 2)就不是正四面体的对称变换.

容易看出，绕任一条过正四面体的一个顶点及其对面中心的轴按逆时针方向旋转 120°、240°的旋转是正四面体的对称变换，这样的变换有 8 个；另一方面，绕任一条过正方体的对边中心的轴旋转 180°的旋转也是正四面体的对称变换，这样的变换有 3 个；再加上恒等变换，共有 12 个对称变换. 所以正四面体至少有 12 个对称变换，且这些变换都是旋转. 又因为镜面反射(1 2)不是正四面体的对称变换，所以镜面反射(1 2)与上述 12 个旋转的乘积也都不是正四面体的对称变换. 由此可知，上述 12 个旋转恰是正四面体的全部对称变换. 这 12 个对称变换用轮换的形式写出就是

(1)，

(1 2 3)，(1 3 2)，(1 2 4)，(1 4 2)，(1 3 4)，(1 4 3)，(2 3 4)，(2 4 3)，

(1 2)(3 4)，(1 3)(2 4)，(1 4)(2 3).

因此，正四面体的对称变换群就是 4 次交代群 A_4. 我们知道，总共存在五种正多面

体.除了正四面体,还有立方体、正八面体、正十二面体和正二十面体.可以求得这几个正多面体的对称变换群的阶数分别是 24、24、60、60,它们分别是 4 次对称群和 5 次交错群.

例 1.4.5 设 $f(x_1,x_2,\cdots,x_n)$是数域K上的一个 n 元多项式,则多项式 $f(x_1,x_2,\cdots,x_n)$的对称变换群等于 S_n 的充分必要条件是 $f(x_1,x_2,\cdots,x_n)$是 n 元对称多项式.

例 1.4.6 试求多项式 $x_1+x_2-x_3-x_4$ 的对称变换群.

解 我们用置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ k_1 & k_2 & k_3 & k_4 \end{pmatrix}$$

表示将 x_i 变到 x_{k_i}的变换,易知,多项式 $x_1+x_2-x_3-x_4$ 的任一置换最多只能将 x_1 与 x_2 或 x_3 与 x_4 互换,所以多项式 $x_1+x_2-x_3-x_4$ 的对称变换群 G 是由(1 2)与(3 4)生成的群,即 $G=\{(1\ 2),(3\ 4)\}$.

从而,$x_1+x_2-x_3-x_4$ 的对称变换群为 $\{(1),(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$.

Euler 小传

欧拉(L. Euler),瑞士数学家、物理学家、天文学家,他 1707 年 4 月 15 日生于瑞士巴塞尔. Euler 于 1722 年在巴塞尔获学士学位,第二年又获硕士学位.对数学有浓厚的兴趣,并得到约翰·伯努利的指导,18 岁起开始发表论文. 1727 年应邀到俄国圣彼得堡科学院工作,1731 年被聘为圣彼得堡科学院物理学教授,1733 年又被聘为该院院士和数学教授.大量的写作使他的右眼在 1735 年因眼疾而失明.

1741 年,Euler 应普鲁士腓特烈大帝的邀请到柏林科学院任物理数学研究所所长,长达 25 年之久. 1766 年回圣彼得堡. 1771 年的一场大病使他的左眼也完全失明,然而他仍凭着惊人的记忆力和心算技巧进行研究,通过口授完成了大量的论著.他的全集有 74 卷之多,他的《无穷小分析引论》、《微分学原理》、《积分学原理》已成为数学中的经典著作.

Euler 的研究几乎涉及数学的每个分支.数学中有许多定理和公式都是以欧拉的名字命名的,如关于多面体的欧拉定理、数论中的欧拉函数、复变函数中的欧拉公式以及微分方程中的欧拉方程等. Euler 早在 1761 年时就给出了群 $U(n)$的例子.

Euler 最突出的数学贡献是扩展了微积分的研究领域,为分析学的一些重要分支与微分几何的产生和发展奠定了基础.他还在代数、数论、组合数学等许多数学领域中有所创建,如发现了实系数多项式的分解定理;给出费尔马小定理的三个证明,并引入了数论中重要的欧拉函数;解决了著名的哥尼斯堡七桥问题等.现在的许多数学符号也起源于欧拉,如用 Σ 来表示求和(1755 年),用 i 表示虚数单位(1777 年),用 e 表示自然

对数的底(1736 年)等.

法国天文学家、物理学家阿拉戈(D. F. J. Arago)称赞欧拉道:"Euler 计算起来轻松自如,就像人们呼吸,鹰在空中飞翔."

Euler 于 1783 年 9 月 18 日卒于俄国圣彼得堡.

问题 1.4

1. 写出正五边形、正六边形的对称变换群 D_5、D_6.
2. 在 D_n 中,用几何方法说明为何两个反射的复合是一个旋转.
3. 在 D_n 中,用几何方法说明为何一个反射与一个旋转的复合是一个反射.
4. 确定 $D_n(n\geqslant 3)$中的元素个数,问 D_n 中有多少个反射?
5. 证明:正方形的对称变换群与多项式$(x_1+x_2)(x_3+x_4)$的对称变换群同构.

第 2 章 群的结构

群论的发生比较早，约在 18 世纪末和 19 世纪初. 起初它仅是为了解决高次方程的根是否能用根号表示的问题而发展起来的. 在解决上述问题中，第一次发现了方程的根的对称性和平等性是解决全部问题的关键. 从 19 世纪到 20 世纪这段时间，在科学的许多别的部门，例如几何、结晶学. 物理、化学都弄清了对称的规律的重要意义，因此群论的方法和结果得到了广泛的应用.

群论是现代数学中最早和最丰富的分支之一. 其中，变换群在几何学中起着一个重要的作用，而有限群是方程论中的 Galois 理论的基础，这两个领域对群论的系统研究提供了原动力.

我们将从比群更一般的概念——半群开始讨论，尽管半群的理论还不像群论那样丰富，然而它有着重要的"对外的"应用，特别值得注意的是对于自动机理论. 虽然我们的主要目标是群的对称理论，但我们还是将从比较简单且更一般的半群概念来开始我们的讨论，期望半群的先行研究能提供一个更好的洞察力来讲清楚关于群的某些结果.

§2.1 群

定义 2.1.1 设集合 S 和 S 上的满足结合律的二元运算 · 所形成的代数系统叫做半群. 这个半群记成 $(S,\cdot)$ 或者简记成 S.

运算 $x\cdot y$ 也常常简写成 xy. 像通常那样令

$$x^2=x\cdot x, x^n=x\cdot x\cdot\cdots\cdot x(n\text{ 个 }x).$$

如果运算又满足交换律，则 $(S,\cdot)$ 叫做可换半群.

定义 2.1.2 设 S 是半群，元素 e 叫做半群的单位元，是指对任意 $a\in S$，$ae=ea=a$. 如果 S 有单位元 e，则它是唯一的，记作 1.

定义 2.1.3 设 S 是含单位元半群，元素 b 叫做元素 a 的逆元素，是指 $ab=ba=1$. 如果 a 有逆元素，则它是唯一的.

我们把这个唯一的逆元素记作 a^{-1}，则 $aa^{-1}=a^{-1}a=1$.

例 2.1.1 $(\mathbf{N},+)$，$(\mathbf{Z},+)$，$(\mathbf{Q},+)$ 都是半群.

例 2.1.2 以 $M_n(C)$表示 n 阶复方阵全体,它对乘法形成含单位元半群,单位元是单位方阵 I_n,并且当 $n\geqslant 2$ 时,易知半群 $M_n(C)$不是交换的.

例 2.1.3 设 n 为正整数,我们在 $\mathbf{Z}$ 上定义如下关系:对于整数 a 和 b,$a\sim b\Leftrightarrow n|a-b$(即 $a\equiv b(\mathrm{mod}n)$)

易知这是等价关系,于是 $\mathbf{Z}$ 拆分成 n 个等价类:$[0],[1],\cdots,[n-1]$,以 $\mathbf{Z}_n$ 表示上述等价类组成的集合,在 $\mathbf{Z}_n$ 上定义乘法:$[a][b]=[ab]$,则 $\mathbf{Z}_n$ 对此乘法是含单位元交换半群,单位元是$[1]$.

在 $\mathbf{Z}_n$ 上定义加法:$[a]+[b]=[a+b]$,则 $\mathbf{Z}_n$ 是含单位元交换半群,单位元是$[0]$.

例 2.1.4 我们已经知道,若有映射 $\alpha:S\to T,\beta:T\to U,\gamma:U\to V$,则$(\alpha\beta)\gamma=\alpha(\beta\gamma)$.由此,设有非空集 S,令 $T(S)=\{\alpha|\alpha$ 是 S 到 S 的映射$\}$,以"·"表示映射的积,则$(T(S),\cdot)$是一个有单位元半群.

定义 2.1.4 设 S 是一个半群,集 S 中的等价关系 ρ 叫做半群 S 上的同余关系,简称同余,是指若 $a\rho c,b\rho d$,则 $ab\rho cd$.

以后,如果 ρ 是半群 S 上的同余,对 $a\in S$,称 a 关于 ρ 的等价类为 a 关于 ρ 的同余类,常以 $a\rho$ 记之,由此得下述命题.

定理 2.1.1 设 ρ 是半群 S 上的同余,在商集 S/ρ 中定义,$(a\rho)(b\rho)=(ab)\rho$,则 S/ρ是一个半群.

证明 由上所述,$(a\rho)(b\rho)=(ab)\rho$ 是 S/ρ 中的运算,由 S 中运算的结合律立即得到 S/ρ 中运算的结合律.常称上述半群 S/ρ 为 S 关于同余 ρ 的商半群.

例 2.1.5 在半群$(\mathbf{Z},+)$中,考虑等价关系"模 $n(n>1)$同余",若 $a\equiv c(\mathrm{mod}n)$,$b\equiv d(\mathrm{mod}n)$,则 $c=a+kn$,$d=b+hn$,故 $c+d=a+b+(k+h)n$,从而 $a+b\equiv c+d(\mathrm{mod}n)$,故模 n 同余是半群$\langle\mathbf{Z},+\rangle$中的同余.相应的商半群正是例 1.1.3 中的半群.

定理 2.1.2 设 ρ 是半群 S 上的同余,则自然映射 $\upsilon:S\to S/\rho$,对 $a\in S$,$a\upsilon=a\rho$,是满同态.

证明 υ 是满射,又$(ab)\upsilon=(ab)\rho=a\rho b\rho=a\upsilon b\upsilon$,从而 υ 是满同态.

定理 2.1.3 设 S 是一个半群,令 $X=S^1$,则存在单同态 $\rho:S\to T(X)$,从而 $S\cong S\rho\leqslant T(X)$.

证明 设映射 $\rho:S\to T(x)$为对 $a\in S$,$a\rho=\rho_a$,其中 $\rho_a:S^1\to S^1$ 为对 $x\in S^1$,$x\rho_a=xa$,则 ρ 是单射.事实上,对 $a,b\in S$,若 $a\rho=b\rho$,则 $\rho_a=\rho_b$.故对$\forall\ x\in S^1$,$xa=xb$.

特别地,令 $x=1$,得 $a=b\rho$ 是一个单同态,这是因为

$x(\rho_a\rho_b)=(x\rho_a)\rho_b=(xa)\rho_b=(xa)b=x(ab)=x\rho_{ab}$,$x\in S$,从而${}_a\rho_b=\rho_{ab}$.

设 S 是半群,E 是集 S 上的一个等价关系,于是商集 $S/E=\{[a]|a\in S\}$,这里$[a]$表示 a 关于等价关系 E 的等价类.在商集中能否借助于 S 中的运算,规定$[a][b]=$

$[ab]$得到S/E中的运算？一般来说是不行的，这是因为一般情况下，$[ab]$依赖于$[a]$中代表元素a及$[b]$中代表元素b的选择，即aEc，bEd不能保证$abEcd$. 这就导致下述关于同余的概念.

定义 2.1.5　非空集合G，“·”是它的运算，如果满足：

i. $\forall a,b\in G$，有$ab\in G$；

ii. 结合律成立，即$\forall a,b,c\in G$，有$(ab)c=a(bc)$；

iii. 存在单位元$e\in G$，即存在一个元e，对于$\forall a\in G$，有$ae=ea=a$；

iv. $\forall a\in G$，a都有逆元a^{-1}，即$aa^{-1}=a^{-1}a=e$.

称G对于其上的运算来说构成了一个群，记为$(G,\cdot)$.

定义 2.1.6　如果群中所含元素个数是有限数n，称为有限群；其元素个数称为群的阶，记为$|G|=n$.

例 2.1.6　$\{1,-1,\mathrm{i},-\mathrm{i}\}$对于普通乘法构成四阶群. 其中1是单位元，$-1$是1的逆元，i与$-$i互为逆元.

例 2.1.7　$S_3=\{(1),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$对于置换的合成构成有限非交换群，称为三次对称群.

例 2.1.8　实数集合$\mathbf{R}$上所有n阶可逆方阵的集合$GL_n(\mathbf{R})$，对于矩阵的乘法构成群，称为一般线性群.

例 2.1.9　考虑群$(\mathbf{Z},+)$，令$n\mathbf{Z}=\{na\,|\,a\in\mathbf{Z}\}$，这里$n$是一个固定$ABCD$，令$R$为该正方形绕中心$O$逆时针方向旋转$90°$的变换，则$R^4=RRRR=E$是恒等变换. 令$H$为正方形$ABCD$对$x$轴的反射，令$V$为正方形$ABCD$对$y$轴的反射，令$D$为正方形$ABCD$对$BD$轴的反射，$D'$为对$AC$轴的反射，则$D_4=\{R_1,R_2,R_3,R_4=E,H,V,D,D'\}$关于变换的积是一个群. $R_4=E$是它的恒等元. D_4叫做二面体群.

例 2.1.10　在$\mathbf{Q}$中规定：$\forall a,b\in\mathbf{Q}$，有$a\cdot b=a+b+ab$，$(\mathbf{Q},\cdot)$是否成群？

解　显然 i. 是成立的；

ii.
$$\begin{aligned}(a\cdot b)\cdot c&=(a+b+ab)\cdot c=(a+b+ab)+c+(a+b+ab)c\\&=a+b+c+ab+ac+bc+abc,\end{aligned}$$
$$\begin{aligned}a\cdot(b\cdot c)&=a\cdot(b+c+bc)=a+(b+c+bc)+a(b+c+bc)\\&=a+b+c+ab+ac+bc+abc,\end{aligned}$$

所以$(a\cdot b)\cdot c=a\cdot(b\cdot c)$；

iii. 如果e是单位元，则对于任意$a\in\mathbf{Q}$，应有$ae=ea=a$，这时$ae=a+e+ae=a$，得$e=0$，所以数0是单位元；

iv. 对于$\forall a\in\mathbf{Q}$，如果b是a的逆元，应有$ab=ba=0$，这时$ab=a+b+ab=0$，得b

$=\dfrac{-a}{1+a}$，a 的逆元是 $\dfrac{-a}{1+a}$，而 -1 没有逆元.

综上所述，$(\mathbf{Q},\cdot)$ 不构成群. 但是，对于 $Q-\{-1\}$ 对上面的乘法"·"就构成群.

定义 2.1.7　设 $(G,\cdot)$ 是一个群，G 的非空子集 A 关于二元运算"·"封闭，且 $(A,\cdot)$ 也是一个群，则称 $(A,\cdot)$ 为群 $(G,\cdot)$ 的子群，并记为 $A\leqslant G$.

例 2.1.11　设 $(G,\cdot)$ 是一个群，令 $C=\{a\mid a\in G, x\in G\Rightarrow xa=ax\}$，则 $C\leqslant G$，C 叫 G 的中心. C 的单位元正是 G 的单位元.

以上例子表明，子群 H 的单位元正是群 G 的单位元. 这一结论是普遍成立的. 事实上，设 $H\leqslant G$，e_H 是 H 的单位元，e_G 是 G 的单位元，在 H 中有 $e_H\cdot e_H=e_H$，但在 G 中有 $e_H\cdot e_G=e_H$，从而在 G 中我们有 $e_H\cdot e_H=e_H\cdot e_G$，由 G 中的消去律得 $e_H=e_G$.

由于 $e_H=e_G$，从而子群 H 中的元素 a 的逆元正是 a 在 G 中的逆元. 由此，我们得到下述定理：

定理 2.1.4　设 $(G,\cdot)$ 是一个群，e 是 G 的单位元，则 G 的子集 H 是子群的充要条件是：

(1) $e\in H$；(2) $a,b\in H\Rightarrow ab\in H$；(3) $a\in H\Rightarrow a^{-1}\in H$.

从这个定理立即得到，若 H_1，H_2 是 G 的子群，则 $H_1\cap H_2$ 也是 G 的子群. 一般地，若 $\{H_i\mid i\in I\}$ 是 G 的子群族，则其交 $\bigcap\{H_i\mid i\in I\}$ 也是 G 的子群.

为了考察各种群之间的联系，我们要研究群之间的映射，但是群不仅是集合还有运算，所以需要映射与群运算保持协调. 确切地说：

定义 2.1.8　设有群 $(G,\cdot)$，$(G',\odot)$，映射 $\mu:G\to G'$ 叫同态，是指对 $\forall\, a,b\in G$ 有 $(a\cdot b)\mu=(a\mu)\odot(b\mu)$.

由此我们可以看到，群的同态正是群作为半群的同态：$\mu:G\to G'$，同态也可以叙述如下：

$$\mu\times\mu:G\times G\to G'\times G'，为 (a,b)(\mu\times\mu)=(a\mu,b\mu).$$

对于同态 μ，如果映射 μ 是单射，则称同态 μ 为单同态；如果映射 μ 是满射，则称同态 μ 为满同态；如果映射 μ 是双射，则称同态 μ 为同构. 如果存在从群 G 到群 G' 的同构，则称群 G 与 G' 同构，记作 $G\cong G'$.

从同态的定义立即得到同态的下述基本性质：

(1) 若 $\mu:G\to G'$ 是群的同态，则 $e\mu=e'$，这里 e，e' 分别是 G，G' 的恒等元.

事实上，$e\mu=(ee)\mu=(e\mu)(e\mu)$，又 $e\mu=(e\mu)e'$，从而由消去律得 $e\mu=e'$.

(2) 若 $\mu:G\to G'$ 是群的同态，$a\in G$，则 $(a^{-1})\mu=(a\mu)^{-1}$.

事实上，$e'=e\mu=(aa^{-1})=(a\mu)((a^{-1})\mu)$，两边左乘 $(a\mu)^{-1}$，得 $(a^{-1})\mu=(a\mu)^{-1}$.

(3) 若 $\mu:G\to G'$ 是群的同态，$a\in G$，$k\in\mathbf{Z}$，则 $(a^k)\mu=(a\mu)^k$.

事实上,当 $k=0$ 时,$a^k=e$,故 $(a^k)\mu=e\mu=e'$;但当 $k=0$ 时,$(a\mu)^k=e'$,从而 $k=0$ 时等式成立;

当 $k>0$ 时,可用归纳法证明.对于 $k<0$ 的情形,可利用性质(2)及 $k>0$ 的结论得到.

(4)若 $\mu:G\to G'$ 是群的同态,则 $G_\mu=\{a\mu|a\in G\}$ 是 G' 的子群,叫做 G 关于 μ 的同态像.

事实上,首先 $e'=e\mu\in G\mu$,若 $a',b'\in G\mu$,则存在 $a,b\in G$ 使 $a'=a\mu,b'=b\mu$,从而 $a'b'=(a\mu)(b\mu)=(ab)\mu\in G\mu$;又 $(a')^{-1}=(a\mu)^{-1}=(a^{-1})\mu\in G\mu$,从而 $G\mu$ 是 G' 的子群.

由此,若 $\mu:G\to G'$ 是同态,H 是 G 的任一子群,将 μ 限制在 H 上,便得到同态 $\mu:H\to G'$,于是 $H\mu$ 是 G' 的子群,从而子群 H 关于 μ 的同态像 $H\mu$ 是 G' 的子群.

例 2.1.12 设有数域 P 上的 n 维向量空间 V,$L_n(V)$ 与 P 上的 n 阶可逆矩阵的集关于矩阵乘法形成的群同构.

从同构的定义立即看到,若 $\alpha:G\to G'$ 是同构映射,则 $\alpha:G'\to G$ 也是同构映射,从而 $G\cong G'\Rightarrow G'\cong G$.又对任一群 G,$I_G:G\to G$,即 G 到自身的恒等映射,显然是一个同构映射,从而对任何群 G,有 $G\cong G$.

又若 $\alpha:G\to G'$,$\beta:G'\to G''$ 都是同构映射,则 $\alpha\beta:G\to G''$ 也是同构映射,从而 $G\cong G''$.由此,$G\cong G',G'\cong G''\Rightarrow G\cong G''$.

定理 2.1.5(Cayley 定理) 任一群必同构于一个变换群.

证明 定义映射 $\rho:G\to \mathrm{Sym}(G)$,对 $a\in G$,$a\rho=\rho_a$,其中 $\rho_a:G\to G$,对 $x\in G$,$x\rho_a=xa$.由定理 2.2.1 知,ρ 为单同态,且 $G\cong G_\rho\leqslant \mathrm{Sym}(G)$.而 G_ρ 是集合 G 上的变换群.

定义 2.1.9 a 是群 G 中一元素,如果存在正整数 n 使得 $a^n=e$,使等式成立的最小的正整数称为元素 a 的周期.

例 2.1.13 $U=\{1,\omega,\omega^2\}$,其中 ω 为 1 的三次单位原根,则 U 对于普通乘法构成群.单位元 1 的周期是 1;ω、ω^2 的周期都是 3;

例 2.1.14 一个 n 元集合的全体置换构成的群称为 n 次对称群,记为 S_n;S_n 的阶数是 $n!$.

定义 2.1.10 设 $G_1,G_2\cdots G_n$ 是任意 n 个群,则称

$$G_1\times G_2\times\cdots\times G_n=\{(a_1,a_2\cdots a_n)\,|\,a_i\in G_i,i=1,2\cdots n\}$$

对于运算:$(a_1,a_2\cdots a_n)(b_1,b_2\cdots b_n)=(a_1b_1,a_2b_2\cdots a_nb_n)$ 作成一个群,称为群 $G_1,G_2\cdots G_n$ 的**直积**.

例 2.1.15 $G_1=(a)$,$G_2=(b)$ 分别为 3 阶和 5 阶循环群,$G=G_1\times G_2$ 为 15 阶循环群.

证明 $G_1=(e_1,a,a^2)$,$G_2=(e_2,b,b^2,b^3,b^4)$,其中 a,b 的周期分别为 3 和 5,在 G 中

取 (a,b)，则 $(a,b)^3=(e_1,b^3)$，$(a,b)^5=(a^2,e_2)$，又 3 和 5 互素，所以 (a,b) 的周期为 15，则 $G=G_1\times G_2$ 为 15 阶循环群.

显然，对称变换所满足的性质与群中元素的运算非常类似，如果我们抛开元素和运算的具体内容和形式，而注重两者之间的本质关系，就能得到下面结论：

群是对称概念的数学描述，研究群就是为了研究复杂的对称.

Cayley 小传

凯莱(A. Cayley)，1821 年 8 月 16 日出生在英格兰，父亲在俄国经商，凯莱的童年在那里度过. 8 岁时随父母返回英国. 14 岁入国王学校学习，数学才华初露，擅长大数运算. 17 岁考入剑桥大学三一学院，20 岁不到就发表了他的第一篇论文，第二年又发表了 8 篇论文. 三一学院毕业后留校任教 3 年.

25 岁时 Cayley 开始了 14 年的律师生涯. 任职期间又发表了近 200 篇数学论文，其中的大部分现已成为经典的数学内容. 1863 年，Cayley 应邀返回剑桥任数学教授，直至去世. 他最大的非数学方面的贡献是由于他的影响使剑桥向妇女开放了. Cayley 和他的好友西尔威斯特(J. J. Sylvester)是不变量理论的奠基人，而不变量理论在以后相对论的研究中起了重要的作用. 他引入了抽象群、群代数以及矩阵等概念，并对几何与线性代数做出了主要的贡献，其中包括：发明了表示行列式的两竖符号，建立行列式的乘法定理等.

Cayley 一生中仅出版过一本专著《椭圆函数初论》(1876)，但发表了近 1000 篇论文，他的论文选集有 13 卷之多，每卷长达 600 多页.

Cayley 于 1895 年 1 月卒于剑桥.

问题 2.1

1. 确定 S_3 的乘法表.

2. 令 G 是用 $x\to x'=ax+b$，其中 a 和 b 都是实数且 $a\neq 0$ 所定义直线 R 的变换的集，验证 G 是 R 的一个变换群.

3. 令 G 是一个半群 M 的一个非空子集，则 G 是一个子群当且仅当每个 $g\in G$ 的 M 中都是可逆的，并且对 $\forall\ g_1,g_2\in G,g_1^{-1}g_2\in G$.

4. 证明：假如 $n\geqslant 3$，那么 S_n 的中心的阶是 1.

5. 设 G 为有限群，$|G|=mn$，$(m,n)=1$，$g\in G$，证明：G 中存在唯一的元素 x 和 y，使得 $g=xy=yx$ 且满足 $x^m=y^n=1$.

6. 设 G 为 n 阶群，$g_1,g_2,\cdots,g_n\in G$，证明：存在整数 i,j，$1\leqslant i\leqslant j\leqslant n$，使得 $g_ig_{i+1}\cdots g_j=1$.

7. 设 G 是群，$K=\{g_1,g_2,\cdots,g_n\}\subseteq G$ 且 $1\notin K^2$，证明：在 n^2 个乘积 g_ig_j 中，至多有 $n(n-1)/2$ 个元素 $g_ig_j\in K$.

8. 设 a,b 是群 G 中两个可交换的元素，证明：$|a|=\dfrac{|a||b|}{(|a|,|b|)}$.

§2.2　置换群

1. 循环群

设 G 是一个群，S 是 G 集的一个非空子集. 常常需要考虑 G 的包含 S 的最小子群，即这样一个子群，它包含 S 而又包含在每一个包含 S 的子群中. 如果这样的子群存在，那么它是唯一的. 这是因为，若 H_1,H_2 是含 S 的最小子群，易知 $H_1\subseteq H_2$，$H_2\subseteq H_1$，故有 $H_1=H_2$. 它的存在性可由下面命题得到.

定理 2.2.1　S 是群$(G,\cdot)$的子集，设 H_i，$i\in I$，是群 G 中含 S 的所有子群，则 $H=\bigcap\{H_i|i\in I\}$是含 S 的最小子群.

证明　首先 G 是含 S 的子群，因而 I 不是空集. 由于 H 是子群，显然 $S\subseteq H$. 若 $S\subseteq H'$ 且 H' 是子群，则 H' 是 H_i 中的某一个，故有 $H=\bigcap\{H_i|i\in I\}\subseteq H'$.

此命题只是肯定含 S 的最小子群 H 的存在性，然而不是构造性的，即对 H 的组成没有什么了解，下面我们从构造的观点，找出含 S 的最小子群 H.

如果 S 是子群，即有 $S\cdot S\subseteq S$，$S^{-1}\subseteq S$，显然此时 $H=S$. 如果 S 是空集，显然$\{e\}$是含 S 的最小子群. 如果 S 非空但不是子群，那么 $a,b\in S$ 存在，使得 $ab\notin S$ 或 $a^{-1}\notin S$，这时我们把这些元素都添加到 S 上去.

$$H=\{x_1x_2\cdots x_n|n\text{ 是自然数},x_i\in S\cup S^{-1}\}.$$

这就是考虑由 S 的元素和 S^{-1}的元素以及由 S 及 S^{-1}中取出任意 n 个元素作乘积所得到的元素全体. 容易证明 $H\cdot H\subseteq H$，$H^{-1}\subseteq H$，即 H 是含 S 的子群. 另一方面，若有子群 $K\supseteq S$，则 $K\supseteq S^{-1}$，令 $S'=S\cup S^{-1}$，即有 $K\supseteq S'$. 这样 K 必包含 $S'\cdot S'$，随之必包含$(S'\cdot S')\cdot S'$，…，故知 $K\supseteq H$，即证得 H 是含 S 的最小子群.

定义 2.2.1　1)群 G 中含 S 的最小子群称为 S 在 G 中生成的子群，记作$\langle S\rangle$；

2)设 H 是群 G 的一个子群. 如果子集 $S\subseteq H$ 且$\langle S\rangle=H$，则称 S 是子群 H 的一个生成元集；

3)特别地，当 $S\subseteq G$ 而$\langle S\rangle=G$ 时，称 S 生成群 G，而 S 是群 G 的一个生成元集.

当 S 是一个有限子集时，我们称 G 为有限生成的. 特别地，当 $S=\{a\}$是由一个元素 a 组成时，我们常以$\langle a\rangle$代替$\langle\{a\}\rangle$(一般地，以$\langle a_1,a_2,\cdots,a_r\rangle$代替$\langle\{a_1,a_2,\cdots,a_r\}\rangle$)，并

称 G 是由 a 生成的循环群. 而称 a 是 G 的生成元. 此时 $G=\langle a\rangle$ 中元素的一般构造是 $a^n, n\in\mathbf{Z}$,从而 $G=\langle a\rangle=\{a^n\mid n\in\mathbf{Z}\}$,显然,它是一个可换群.

定理 2.2.2　如果 G 是一个循环群,则 G 必有下列形状:

1) $G=\{\cdots,a^{-n},\cdots,a^{-2},a^{-1},e,a,a^2,\cdots,a^m,\cdots\}=\{a^n\mid n\in\mathbf{Z}\}$,

其中 $a^n=a^m\Leftrightarrow n=m$;

2) $G=\{e,a,a^2,\cdots,a^{n-1}\}$;其中 $a^n=e$,而 $a^s=a^t, 0\leqslant s,t\leqslant n-1\Leftrightarrow s=t$;

证明　G 是循环群,故有 $G=\langle a\rangle, a\in G$.

若 a 的周期是 ∞,则对任意整数 n,m,若 $n\neq m$,必有 $a^n\neq a^m$. 否则,若 $a^n=a^m$,则有 $a^{n-m}=a^na^{-m}=a^ma^{-m}=e$,这与 a 的周期是 ∞ 矛盾,便得 1)的情形.

若 a 的周期是 n,则 $\{e,a,a^2,\cdots,a^{n-1}\}$ 由 n 个不同元素(证明!)组成且关于乘法和取逆(例如 $a^{-1}=a^{n-1}$, $(a^s)^{-1}=a^{n-s}$)是封闭的,即它是含 a 的子群,故有

$G=\langle a\rangle=\{e,a,a^2,\cdots,a^{n-1}\}$ 而得命题中的 2).

这个命题说明如果存在循环群 G 的话,那么 G 一定是那种样子,但这完全不能说明循环群确实存在的. 下面的例子说明这两种形状的循环群都存在.

例 2.2.1　$(\mathbf{Z},+)$ 是无限循环群,1,-1 都是生成元.

例 2.2.2　令 U_n 是 1 的 n 次根的乘法群,

令 $\theta=\dfrac{2\pi}{n}$,则 $U_n=\{\alpha^{\frac{2k\pi}{n}i}\mid k=0,1,\cdots,n-1\}=\langle\alpha^{\theta i}\rangle$ 是一个循环群.

例 2.2.3　$(\mathbf{Z}_n,+)$ 是一个 L^n 阶循环群,因为 $(Z_n,+)$ 有单位元 $[0]$, $\mathbf{Z}_n$ 中每个元有逆元,即 $\forall\ [a]\in\mathbf{Z}_n$,存在 $-[a]\in\mathbf{Z}$ 使得 $[a]+[-a]=[0]$.

这样,我们有一个无限循环群 $(\mathbf{Z},+)$ 和一个 n 阶循环群 U_n.

另一方面,任意取一个循环群 G,则有

$$G=\{\cdots,a^{-n},\cdots,a^{-2},a^{-1},e,a,a^2,\cdots,a^n,\cdots\},$$

这时,直接验证知

$$f_1:\mathbf{Z}\to G\qquad m\longmapsto a^m$$

是群 $\mathbf{Z}$ 到群 G 的一个同构对应;或有 $G=\{e,a,a^2,\cdots,a^{n-1}\}$,可直接验证

$$f_2:U_n\to G\qquad e^{\theta i}\longmapsto a^i,\qquad i\in\{0,1,2,\cdots,n-1\}$$

是群 U_n 到群 G 的一个同构对应.

如果把同构的群看成相同的,总结一下上面的讨论就有

定理 2.2.3　循环群有且仅有 $(\mathbf{Z},+)$ 和 $U_n, n\in\mathbf{N}$.

循环群是一类最简单的群. 对循环群来说,很多关于群的基本问题都比较容易解决,例如,确定一个给定群的所有子群,这对一般群来说是一个很难解决的问题,但对于循环群来说却很容易解决.

定理 2.2.4 循环群的子群都是循环群. 设 $G=\langle a\rangle$ 是循环群.

(1)若 G 是无限循环群,则对每个正整数 m,G 恰有一个指数为 m 的子群 $G_m=\langle a^m\rangle$,并且它们和 $\{1\}$ 是 g 的全部子群.

(2)若 G 是 n 阶有限循环群,则对 n 的每个正因子 m,G 恰有一个指数为 m 的 n/m 阶子群 $G_m=\langle a^m\rangle$,并且它们是 G 的全部子群.

证明 设 H 是 $G=\langle a\rangle$ 的子群. 不妨设 $H\neq\{1\}$,令 m 是满足 $a^m\in H$ 的最小正整数,易知对每个整数 n,$a^n\in H\Leftrightarrow m\mid n$,于是 $H=\langle a^m\rangle=G_m$,并且当 a 为无限阶元素时,$[G:G_m]=m$. 这就证明了(1).

若 a 是 n 阶元素,则 $m\mid n$(设 $n=mq+r$,$0\leqslant r\leqslant m-1$,$q\in\mathbf{Z}$,由 $a^m\in H$ 可知 $a^r=a^{n-mq}=(a^m)^{-q}\in H$. 由 m 的极小性可知 $r=0$,即 $m\mid n$),于是 $n=mq$. 从而

$$H=G_m=\{1,a^m,a^{2m},\cdots,a^{(q-1)m}\}.$$

这是 $q=n/m$ 阶循环群,从而 $[G:G_m]=|G|/|G_m|=n/q=m$. 这就证明了(2).

2. 置换群

除了同态基本定理,研究群的另一个重要手段是群在集合上的作用,或者说成是群的置换表示,即一个给定群到某个置换群上的同态. 为此,我们在本节介绍有限集合上置换群的基本知识.

设 S 是非空集合,集合 S 到自身的每一个一一对应叫做 S 上的一个置换. 以 $A(S)$ 表示 S 上全部置换构成的集合. 在合成运算 $f\circ g$ 之下,$A(S)$ 是群,因为合成满足结合律,两个置换的乘积仍是集合上的置换,1_S 是恒等置换,并且每一个置换都有逆,$A(S)$ 叫做 S 上的对称群,它的每个子群均叫集合 S 上的置换群.

设 S 和 S' 是两个有限集合,如果 $|S|=|S'|=n$,易知 $A(S)$ 和 $A(S')$ 同构,从而可以谈 n 元集合上的对称群,表示成 S_n,且 $|S_n|=n!$. 而 S_n 的每个子群均叫 n 元集合上的置换群.

我们以 $(i_1\,i_2\cdots i_r)$ 表示如下的置换:

$$i_1\to i_2,i_2\to i_3,\cdots,i_r\to i_1$$

把 $(i_1i_2\cdots i_r)$ 叫做一个长为 r 的轮换. 由此,每个置换均可写成一些轮换的乘积,使得不同的轮换中没有相同元素. 例如

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&6&7&1&2&4&8\end{pmatrix}=(1\ 5)(2\ 3\ 6)(4\ 7)(8).$$

长为 1 的置换常常略去不写,即上式记为 $(1\ 5)(2\ 3\ 6)(4\ 7)$. 如果不同轮换中没有相同元素,这些轮换的次序可任意改变.

例如,$(1\ 5)(2\ 3\ 6)(4\ 7)=(2\ 3\ 6)(1\ 5)(4\ 7)=(4\ 7)(1\ 5)(2\ 3\ 6)$.

因此除次序不同外,置换表示成没有共同数字的轮换之积是唯一的. 长为 2 的轮换叫对换.

容易看到,每个轮换可表成一些对换之积.

例如 $(i_1 i_2 \cdots i_r)=(i_1\ \ i_2)(i_1\ \ i_3)\cdots(i_1\ \ i_r)$,所以每个置换总可表成有限个对换之积. 这种表达式(乃至对换的个数)显然不唯一,但是,同一个对换以多种方式表成对换之积时,其所含对换个数的奇偶性是不变的. 表成奇(偶)数个对换之积的置换叫做奇(偶)置换.

显然,两个奇置换或偶置换之积是偶置换,一个奇置换与一个偶置换之积是奇置换.

全体偶置换构成的子群叫做 n 元集合上的**交**错群 A_n.

易知 A_n 是 S_n 的正规子群,并且$[S_n : A_n]=2$,$|A_n|=n!/2(n\geqslant 2)$.

定义 2.2.2　只有平凡正规子群的群叫做单群.

素数阶群 $\mathbf{Z}_p$ 是循环群,它只有平凡子群$\{1\}$和 $\mathbf{Z}_p$,从而是单群. 元素个数大于 1 的群是单群的充要条件是它为素数阶(循环)群.

定理 2.2.5　当 $n\geqslant 5$ 时,交错群 A_n 是单群.

我们要给出的证明是非常初等的. 首先需要两个引理.

引理 2.2.6　当 $n\geqslant 3$ 时,长为 3 的轮换形成 A_n 的一个生成元系.

证明　设 $\sigma\neq 1$ 是偶置换,则 σ 是偶数个对换之积. 从而只需证任意两个对换之积可用长为 3 的轮换表示即可.

对于$\tau=(ij)(rs)(i\neq j,r\neq s)$. 如果$(ij)=(rs)$,则 $\tau=1$. 如果 $j=r,i\neq s$,则 $\tau=(jsi)$. 如果 i,j,r,s 两两不等,则 $\tau=(ris)(ijr)$.

引理 2.2.7　如果 N 是 $A_n(n\geqslant 3)$的正规子群,并且 N 包含一个 3-轮换,则 $N=A_n$.

证明　如果$(rsc)\in N$,则对每个 $k\neq r,s,c$,$(rsk)=(rs)$.

$$(ck)(rsc)^2(ck)(rs)=[(rs)(ck)](rsc)^2[(rs)(ck)]^{-1}\in N.$$ 知 $N=A_n$.

定理 2.2.5 的证明　设$\{1\}\neq N\lhd A_n$,我们证明 $N=A_n$.

N 中必包含一个元素是长为 3 的轮换. 事实上,设 $1\neq\sigma\in N$,并且 σ 将$\{a_1,\cdots,a_n\}$中尽可能多的元素保持不动. 我们把 σ 恰好变动 3 个 a_i,从而必是长为 3 的轮换. 首先,σ 至少变动 3 个 a_i(因为只变动两个 a_i 的为对换,而对换是奇置换,不属于 A_n),现在把 σ 写成没有公共元素的轮换之积,并且把最长的轮换写在左边. 若 σ 恰好变动 4 个 a_i,则 $\sigma=(a_1\ a_2)(a_3\ a_4)$. 由于 $n\geqslant 5$,从而 $\beta=(a_3 a_4 a_5)\in A_n$,而

$$\sigma_1=\beta\sigma\beta^{-1}=(a_1\ a_2)(a_4\ a_5)\in N,$$

于是

$$\sigma\sigma_1=(a_3\ a_4)(a_4\ a_5)=(a_3\ a_4\ a_5)\in N,$$

即是长为 3 的轮换. 若 σ 至少变动 5 个 a_i，则又分三种情形考虑：

1）σ 包含长度$\geqslant 4$的轮换，即 $\sigma=(a_1a_2a_3a_4\cdots)\cdots$. 取 $\beta=(a_2a_3a_4)\in A_n$，则 $\sigma_1=\beta\sigma\beta^{-1}=(a_1a_3a_4a_2\cdots)\cdots\in N$，而 $i\geqslant 5$ 时，$\sigma(a_i)=\sigma_1(a_i)$，从而 N 中 $\sigma_1\sigma^{-1}$至多变动 4 个 a_i，这与 σ 变动 a_i 个数的极小性矛盾；

2）σ 中轮换最大长度为 3，则 $\sigma=(a_1\ a_2\ a_3)(a_4\ a_5\cdots)\cdots$，由于 σ 至少变动 5 个 a_i，从而 σ 不是长为 3 的轮换，则 σ 至少变动 6 个 a_i. 取 $\beta=(a_2\ a_3\ a_4)\in A_n$，则

$$\sigma_1=\beta\sigma\beta^{-1}=(a_1\ a_3\ a_4)(a_2\ a_5\cdots)\cdots\in N,$$

而 N 中置换 $\sigma_1\sigma^{-1}$至多变动 5 个 a_i，这又导致矛盾；

3）设 σ 是一些对换之积：$\sigma=(a_1\ a_2)(a_3\ a_4)\cdots$，它至少变动 6 个 a_i. 取 $\beta=(a_2\ a_3\ a_4)\in A_n$，则 $\sigma_1=\beta\sigma\beta^{-1}=(a_1\ a_2)(a_4\ a_5)\in N$，而 $\sigma\sigma_1^{-1}(\in N)$只变动 4 个 a_i，矛盾；

综上可知，N 中包含元素是长为 3 的轮换，即知 $N=A_n$.

Abel 小传

阿贝尔(N. H. Abel)是 19 世纪最伟大的数学家之一。1802 年 8 月 5 日 Abel 出生于挪威，16 岁时，就开始学习牛顿、欧拉、拉格朗日和高斯的经典数学著作. 在他 18 岁那年，他父亲去世，生活的重担从此就压在了他的身上. Abel 一边当私塾老师，并接一些杂活，一边还继续做着他的数学研究. 19 岁时，他解决了一个让一些著名数学家烦恼了数百年的难题，他证明了虽然一元二次、三次甚至四次方程都有求根公式，但是对于一般的五次方程却不存在这样的求根公式！

虽然 Abel 在近世代数的许多研究领域建立起来之前就早早地过世了，但是他对于五次方程求解问题的解决为这些研究领域做出了基础性的工作，此外，他还在椭圆函数论、椭圆积分、Abel 积分以及无穷级数等方面做出过杰出的贡献. 正当 Abel 的工作开始受到应受到的重视时，Abel 染上了肺结核，于 1829 年 4 月 6 日不幸逝世，年仅 27 岁. 1872 年，若尔当(C. Jordan)引入了 Abel 群这一术语，以纪念这位英年早逝的天才数学家.

问题 2.2

1. 证明：恰有一个极大子群的 n 阶群 G 一定是循环群.

2. 设 $G=(a)$是 30 阶的循环群，定义 $\varphi(n)=a^n$，则 φ 是 $\mathbf{Z}$ 到 G 的同态映射. 确定(1)Kerφ；(2)找出与子群$(30)\leqslant(15)\leqslant(5)\leqslant Z$ 对应的 G 的子群.

3. 证明：n 阶群 G 是循环的$\Leftrightarrow$对$\forall\ d|n$，G 有且仅有一个 d 阶循环子群.

4. 设 H 是群 G 的子群，且 H 含于 G 的中心，如果商群 G/H 是循环群，证明 G 是

交换群.

5. 证明:假如 $n\geqslant 3$,那么 A_n 可由 3-循环$(a\ b\ c)$生成.

6. 证明:S_n 可由 $n-1$ 个对换$(1\ 2),(1\ 3),\cdots,(1\ n)$生成,也可由 $n-1$ 个对换$(1\ 2),(2\ 3),\cdots,(n-1\ n)$生成.

7. 证明:交代群 A_4 没有 6 阶子群.

8. 设 $K_4=\{(1),(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$,求证:$K_4\lhd S_4$,且 $S_4/K_4\cong S_3$.

9. 求对称群 S_3 的自同构群 $\mathrm{Aut}S_3$.

10. M 是群 G 的全体子群的集合,定义 G-集 M:对$\forall\ g\in G$ 和 $H\in M$,规定 $g\times H=ghg^{-1}$,求证:$H\in M$ 是 G 的正规子群当且仅当 H 的对称群 $S_H=G$.

§2.3 群的重排定理、正规子群和商群

本节将给出群的几个重要性质.

定理 2.3.1(群的重排定理) 设 g 为群 G 中任意确定元素,则 $Gg=Gg=G$.

证明 因 $g\in G$,故 $g^{-1}\in G$. $\forall\ g_i\in G$,则 $b\equiv g^{-1}g_i\in G$,且 $gb=g_i\in G$(见上节子群充要条件). 但 $gb=g_i\in G$,因此 $gG\supset G$. 又$\forall\ gg_i\in gG$,因为 $g\in G,g_i\in G$,故 $gg_i\in G$,结果 $G\supset Gg$,最后有 $gG=G$.

仿此可证 $Gg=G$.

重排定理是群的最重要、最普遍的性质.

对于有限群,设 $G=\{g_1,g_2,\cdots g_n\}$,集合 gG. 只是把元素重新排列为$\{gg_1,gg_2,\cdots gg_n\}$,定理由此得名.

重排定理还可以推广.

设有群函数 $f(g_i)$,其"数值"(或表示的操作结果)依赖于群元素,则对于任意给定群元素 $g\in G$,有

$$\sum_{g_i\in G}f(g_i)=\sum_{g_i\in G}f(gg_i),\text{或}\sum_{g_i\in G}f(g_i)=\sum_{g_i\in G}f(g_ig)$$

对于有限群,为了更清楚地显示群的乘法结构,常常构造群表,即群的乘法表. 构造规则是,表的第一列排放乘法的第一因子,表的第一行排放乘法的第二因子. 列与行的元素应遍及全部群元素.

例 2.3.1 群 $G=(1,-1,\mathrm{i},-\mathrm{i})$,群运算为普通乘法,则群表如表 2.1 所示.

表 2.1　群表

列 \ 行	1	−1	−i	i
1	1	−1	−i	i
−1	−1	1	i	−i
i	i	−i	1	−1
−i	−i	i	−1	1

例 2.3.2　群 $C_{3V}=(C_3^1,C_3^2,C_3^3=E;m_a,m_b,m_c)$，群运算为连续操作，其中 m_a,m_b,m_c 分别为等边三角形绕过 A 点、B 点和 C 点的垂线转动 180°的操作，则群表如表 2.2 所示.

表 2.2　群表

列元素 \ 行元素	E	C_3^1	C_3^2	m_a	m_b	m_c
E	E	C_3^1	C_3^2	m_a	m_b	m_c
C_3^2	C_3^2	C_3^2	C_3^1	m_b	m_c	m_a
C_3^1	C_3^1	E	E	m_c	m_a	m_b
m_a	m_a	m_c	m_b	E	C_3^1	C_3^2
m_b	m_b	m_a	m_c	C_3^2	E	C_3^1
m_c	m_c	m_b	m_a	C_3^1	C_3^2	E

在构造此表时，我们只应用了群元与群运算定义，如 $m_a \cdot C_3^1=m_c$ 可以直观表示为

$m_a \cdot C_3^1$：



图 2.1

m_c：

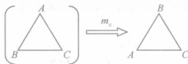


图 2.2

注意到群表中的每一列或每一行，每个群元素都会在其中出现且只出现一次，只是每一列(或行)的群元顺序不同罢了. 在这两个例子中，群表的对角元素均为单位元 E. 在一般构成群表时，并不要求这一点，只是在以后应用(如寻找正则表示)中这种特殊形式的群表(正则形式，或称正则群表)特别方便.

定义 2.3.1 设子群 $H:(h_1,\cdots,h_m)\subset G$，且 $g\in G$，则集合

$$gH=(gh_1,gh_2,\cdots,gh_m)$$

称为元素 g 生成的子群 H 的左陪集，而集合

$$Hg=(h_1g,h_2g,\cdots,h_mg)$$

则称为元素 g 生成的子群 H 的右陪集.

显然，陪集元素的阶与子群 H 的阶相同，但一般来说 $gH\neq Hg$.

陪集的最重要性质可由下述陪集定理表示之.

定理 2.3.2(陪集定理) 同一子群的两个左(或右)陪集，或者元素完全相同，或者完全不同(交集为空集).

证明 若 H 为群 G 的子群，且 g_1 和 g_2 为群 G 中任意给定元素，它们生成的两个左陪集分别是 g_1h 和 g_2h. 设两陪集有一公共元素：

$$g_1h_i=g_2h_j$$

(不要求 $h_i=h_j$，但 h_i、$h_j\in H$)，则两边都乘以 $g_2^{-1}(\cdots)h_i^{-1}$，得

$$g_2^{-1}g_1=h_jh_i^{-1}\in H,$$

由重排定理 $g_2^{-1}g_1H=H$，亦即 $g_2H=g_2(g_2^{-1}g_1H)=g_1H$.

换言之，两个左陪集只要有一个公共元素，就一定是同一集合.

进一步有

定理 2.3.3(Lagrange 定理) 群 G 必为子群 H 及其全部不相同的陪集的直和，即群 G 的阶 n 必为子群 H 的阶 k 的整数倍.

证明 任取 $g_1\in G$，但 $g_1\notin H$，则由陪集定理

$$(H=EH,E\neq g_1),H\cap g_1H=\varnothing.$$

继续取 $g_2\in G$，但 $g_1\notin H\cup g_1H$，则陪集 g_1H，必有

$$g_2H\cap H=\varnothing;g_2H\cap g_1H=\varnothing,$$

则 g_2h 应与 H 或 g_1h 全部重合，与假设矛盾. 如此继续作陪集，因 G 为有限群，必然经过有限次(设为 m 次)后终结，即

$$G=H\cup g_1H\cup g_2H\cup\cdots g_mH,$$

其中每一个左陪集的元素个数均为 k. 陪集的个数为 m 个，故有 $n=mk$.

推论 2.3.4 素数阶群只有平凡子群(群自身与单位元).

共轭类是对群元的另一种分类方法. 共轭关系是群元之间的等价关系. 集合 $W=$

$\{A,B,C\cdots\}$中任意两元素之间，若满足下述三个公设，则称它们之间具有等价关系，记为～：

(1)自反性(反射性) $A\sim A$.

(2)对称性 若 $A\sim B$，则 $B\sim A$.

(3)传递性 若 $A\sim B, B\sim C$，则 $A\sim C$.

在集合中互相等价的元素可归为一类，称为等价类. 由于传递性，不同等价类的元素决不会相同，即不同等价类互不相交. 因此，集合可分解为互不相交的等价类的并集.

定义 2.3.2 对于群 $G=\{g_1,g_2\cdots\}$及$\forall\ g_1,g_2\in G$，若存在元素 $g\in G$，满足 $g_j=g^{-1}g_ig$，则称元素 g_i 与 g_j 共轭.

容易验证共轭关系是一种等价关系，即具有自反性、对称性和传递性. 借此我们可以对群进行共轭分类，即分解为共轭类的并集.

例 2.3.3 对于 C_{4v}群，$(C_4^1)^{-1}\sigma_\mu C_4^1=\sigma_\nu$，即 $\sigma_\nu\sim\sigma_\mu$. 由于$(C_4^1)^{-1}=C_4^3\in C_{4v}$，所以又有 $\sigma_\mu=(C_4^3)^{-1}\sigma_\nu C_4^3$，故 $\sigma_\nu\sim\sigma_\mu$.

例 2.3.4 Abel 群 $G=\{g_1,g_2\cdots,g_i,\cdots\}$. 由于$\forall\ g_ig_j=\in G$，有 $g_ig_j=g_jg_i$，因此 $g_j=g^{-1}g_ig$，即 Abel 群群元只与自身共轭，每一个共轭类只有 1 个群元.

实际上给定共轭类中一个元素 g，即可由 $a_i^{-1}ga_i(\forall\ a_i\in G)$，当 a_i 遍及全部群元，并归并相同元素，就可得到 g 所属的共轭类. 由 1 个元素构成的共轭类，相应元素称为群的中心元素. 任意群的单位元 E 自成一类. 所有中心元素的集合称为群的中心. Abel 群的中心即为自身.

例 2.3.5 C_{4v}群可分为 5 个共轭类：

$$(E);\quad (C_4^2);\quad (C_4^1,C_4^3);\quad (m_\nu,m_\mu);\quad (\sigma_\nu,\sigma_\mu).$$

其中心应为 E, C_4^2 所构成的集合.

一般来说，共轭类不是很容易就可得到的. 后面要讲如何得到群的共轭类. 在这里仅介绍操作群(点群)的共轭类的三个判别方法，在实用中甚为有效.

判别方法 1 不同角度的旋转一般属于不同的类. 如 C_{4v}中 C_4^1、C_4^2 就属于不同类.

判别方法 2 绕某轴旋转某一角度与绕同一轴逆向旋转同一角度，当且仅当群中存在某变换，使转轴反向时，这两个旋转属于同一类. 如在 C_{4v}群中，C_4^1 与 $C_4^3=(C_4^1)^{-1}\equiv C_4^{-1}$. 因为群中存在许多元素 $\sigma_\nu,\sigma_\mu,m_\nu,m_\mu$，均可使转轴反向，故在 C_{4v}中 C_4^1 与 C_4^2 属于同一类.

判别方法 3 或绕两不同轴旋转同一角度，或相对两平面的反射，当且仅当群中存在变换，使得其中一个轴可变换为另一轴，或其中一个平面可变换为另一平面时，这两个旋转属于同一类. 例如 m_ν 和 m_μ，σ_μ 和 σ_ν，，在 C_{4v}群中存在变换使 X 轴变到 Y 轴，一条对角线变到另一条对角线. 如元素 C_4^1.

判别方法 1 与判别方法 2 的证明比较简单，我们证明判别方法 3.

证明　设操作$\hat{a}_1,\hat{a}_2,\hat{q}\in G$，其中$\hat{a}_1,\hat{a}_2$分别表示绕 m、n 轴转动 α 角，$\hat{q}$表示变换 m 轴→n 轴.

如图 2.3 所示，$a'=\hat{a}_1 a, b'=\hat{a}_2, b'=\hat{q}a'$. 显然$\hat{a}=\hat{a}_1 a$，同时

$$b'=\hat{q}a'\Rightarrow a'=\hat{q}^{-1}b'\Rightarrow a'=\hat{q}^{-1}\hat{a}_2 b\Rightarrow a'=\hat{q}^{-1}\hat{a}_2\hat{q}a.$$

由此对比有 $\hat{a}_1=\hat{q}^{-1}\hat{a}_2\hat{q}$，$\hat{a}_1\sim\hat{a}_2$.

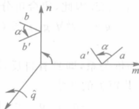


图 2.3

如果子群 H 包含群 G 的完整的共轭类，则称为正规子群或不变子群. 也就是说，$\forall\ h_j\in H, \forall\ X\in G$，有 $h_i=X^{-1}h_j X\in H$.

定义 2.3.3　正规子群是一类特殊的重要子群，其最重要的性质就是它生成的所有左陪集与右陪集相同，即$\forall\ g\in G$，有 $gH=Hg$.

证明　由定义，$\forall\ h_i,h_j\in H, g\in G, gh_i=h_j g$. 当 h_i 遍及子群全部元素，就得到左陪集 gH. 相应地，h_j 遍及 H 全部元素，应得到右陪集 Hg. 否则设左陪集与右陪集不相等，各自至少应有一个元素 $gh_i\neq h_j g$，就有 $h'_i\neq g^{-1}h'_j g$，即 H 未包含完整的共轭类元素. 对于正规子群，可以不必区分左、右陪集. 一般说来，陪集并非群.

群 G 本身与单位元都是平凡正规子群；Abel 群的任何子群都是正规子群.

为了完成对群的结构分解，我们先定义陪集乘法，以便给出商群的定义. 两陪集相乘的法则是，两陪集的所有元素按顺序两两相乘，相同的元素合并为一个，所得到的新的集合称为陪集的乘积.

例 2.3.6　对于群 C_{4v}，子群 $H=(E,C_4^2)\equiv K_1$ 包含完整共轭类，故是正规子群. 另有陪集

$$K_2\equiv C_4^1 H=(C_4^1,C_4^3),$$

$$K_3\equiv m_\chi H=(m_\chi,m_\gamma),$$

$$K_4\equiv\sigma_\mu H=(\sigma_\mu,\sigma_\nu).$$

可以验证“其他陪集”均与上述 4 个陪集重合，由拉格朗日定理，$n=8,k=2,m=4$，已完成陪集分解，陪集相乘，如

$K_3K_4 \Rightarrow (m_\chi, m_\gamma)(\sigma_\mu, \sigma_\nu) \Rightarrow (m_\chi\sigma_\mu, m_\chi\sigma_\nu, m_\gamma\sigma_\mu, m_\gamma\sigma_\nu) \Rightarrow (C_4^3, C_4^1, C_4^1, C_4^3)$

合并之得

$(C_4^1, C_4^3) = K_2.$

可以验证有如表 2.3 所示结果。

表 2.3

X	K_1	K_2	K_3	K_4
K_1	K_1	K_2	K_3	K_4
K_2	K_2	K_1	K_4	K_3
K_3	K_3	K_4	K_1	K_2
K_4	K_4	K_3	K_2	K_1

定义 2.3.4　若 H 为群 G 的正规子群，则 H 与其全部不相同的陪集，在上述陪集乘法定义下，构成一个群，称为商群，记如 G/H.

证明　单位元 H. 设 $\forall\ X \in G$,

$$(XH)H = XH^2 = XH, \quad H(XH) = XHX = XH^2 = XH \quad (\forall\ X \in G).$$

逆元. $\forall\ X \in G$, XH 的逆元为 $X^{-1}H$. 显然，$\forall\ X \in G$，故 $X^{-1}H$ 亦在陪集集合中. $(X^{-1}H)(XH) = XX^{-1}H^2 = H. \quad (XH)(X^{-1}H) = XX^{-1}H^2 = H.$

封闭性. $\forall\ X, Y \in G$，有 $(XH)(YH) = XYH^2 = XYH = ZH$，

其中 $Z = XY \in G$，集合 ZH 应属所说陪集集合.

结合律. $\forall\ X, Y, Z \in G$

$$XH \cdot (YH \cdot XH) = (XH)XYH = XH(YX)H$$
$$= X(XY)H = (XY)XH = (XH \cdot YH) \cdot XH.$$

在上例中，集合 $K = (K_1 = H, K_2, K_3, K_4)$ 就是群 C_{4v} 与 $H = (E, C_4^2)$ 的商群.

例 2.3.7　群 $G = \{1, -1, \mathrm{i}, -\mathrm{i}\}$,

正规子群 $H = \{1, -1\}$, $K = \{\mathrm{i}, -\mathrm{i}\}$，其商群 $G/H = \{H, K\}$

无论对有限群，还是无限群，共轭类、陪集、正规子群、商群的概念依然是有效的.

一个群的全部元素有可能通过群中的几个元素相乘得到. 能够生成全部元素所需的最少群元集合，称为该群的生成元. 有限群或分立群的生成元比较简单，群元通过生成元有限次相乘即可得到. 对于连续群就复杂多了，一般要生成元无限次相乘，才可得到全部群元.

例 2.3.8　对于 C_{4v} 群，生成元可以有如下许多种选择：

$(C_4^1, \sigma_\mu), (C_4^1, \sigma_\nu), (C_4^1, m_\chi), (C_4^1, m_\gamma),$

$(C_4^3, \sigma_\mu), (C_4^3, \sigma_\nu), (C_4^3, m_\chi), (C_4^3, m_\gamma),$

等等. 可见生成元的选择并非唯一的，但是任何选择，每组生成元个数均相同(本例为 2

个).

例 2.3.9　群 $G=\{1,-1,\mathrm{i},-\mathrm{i}\}$,生成元有两种选择(i),(−i).

例 2.3.10　二维旋转群$\{A(\theta)\}$.

$$A(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix},$$

其中 θ 为实参数,其单位元

$$A(0)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

群运算为普通矩阵乘法.读者容易验证$\{A(\theta)\}$满足群的四公理.此时群的生成元

$$X_\theta=\left[\frac{\partial A}{\partial\theta}\right]_{\theta=0}=\begin{pmatrix}-\sin\theta & \cos\theta\\ \cos\theta & \sin\theta\end{pmatrix}_{\theta=0}=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},$$

一般群元可由 X_θ生成

$$A(\theta)=\mathrm{e}^{\theta X_\theta}=E+\theta X_\theta+\frac{1}{2!}\theta^2X_\theta^2+\cdots+\frac{1}{n!}\theta^nX_\theta^n+\cdots(\text{矩阵函数泰勒展开}).$$

由于

$$X_\theta=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},X_\theta^2=\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=-E,$$

$$X_\theta^3=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}=-X_\theta,X_\theta^4=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=E,\cdots$$

故

$$\begin{aligned}A(\theta)&=\left[E+\frac{1}{2!}\theta^2X_\theta^2+\frac{1}{4!}\theta^4X_\theta^4+\cdots\right]+\left[\theta X_\theta+\frac{1}{3!}\theta^3X_\theta^3+\frac{1}{5!}\theta^5X_\theta^5+\cdots\right]\\&=\left[E-\frac{\theta^2}{2!}E+\frac{\theta^4}{4!}E-\cdots\right]+\left[X_\theta\theta-\frac{\theta^3}{3!}X_\theta+\frac{\theta^5}{5!}X_\theta-\cdots\right]\\&=E\left[1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}-\cdots\right]+X_\theta\left[\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\cdots\right]\\&=E\cos\theta+X_\theta\sin\theta\\&=\begin{pmatrix}\cos\theta & 0\\ 0 & \cos\theta\end{pmatrix}+\begin{pmatrix}0 & -\sin\theta\\ \sin\theta & 0\end{pmatrix}=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}.\end{aligned}$$

定理 2.3.5　设 G 是一个群,η 是 G 中的一个同余关系,则等价类 $K=e\eta$ 是 G 的一个正规子群,且对$\forall\ a\in G,a\eta=aK=Ka$;反之,若 K 是 G 的一个正规子群,今定义 G 中的关系 η 为 K_ρ 等价,则 η 是一个同余关系,且由这个同余关系确定的等价类 $a\eta=aK=Ka$.

证明　定理的前半部分已如上所述.下面证明定理的后半部分.设 $a\eta a'$,$b\eta b'$,则存在 $k_1,k_2\in K$,使 $a'=ak_1,b'=bk_2$,于是 $a'b'=(ak_1)(bk_2)$.但 K 是正规子群,故 $bK=Kb$.

从而对 $k_1b\in Kb$，存在 $k_3\in K$，使 $k_1b=bk_3$.

于是 $a'b'=(ak_1)(bk_2)=a(k_1b)k_2=a(bk_3)k_2=ab(k_3k_2)$，故 $a'b'\eta ab$. 从而 η 是一个同余关系. 对这个同余关系，

$$a\eta=\{b\mid b=ak,k\in K\}=\{ak\mid k\in K\}=Ak=Ka.$$

设 $K\lhd G$，则对 $\forall\ a\in G$，左、右陪集 aK，Ka 是相同的，以后我们统称为陪集.

若 $K\lhd G$，η 为 K_λ 等价，于是得到群 $\{G/\eta,\cdot\}$，记作 G/K，并称为 G 关于正规子群 K 的商群. 这样，G/K 中的元素是陪集 $aK(=Ka)$，乘法规则是 $(aK)(bK)=(ab)K$，$K=eK$ 是 G/K 的恒等元，$(aK)^{-1}=a^{-1}K$.

最后我们再给出判断一个子群 H 是否为正规子群的判别准则.

定理 2.3.6　对 G 的子群 H，$H\lhd G\Leftrightarrow$ 对 $\forall\ a\in G$，有

$$a^{-1}Ha=\{a^{-1}ha\mid h\in H\}\subseteq H.$$

证明　$\Rightarrow$ 因为 $H\lhd G$，故对 $\forall\ a\in G$，有 $aH=Ha$. 设 $a^{-1}ha\in a^{-1}Ha$，则 $h\in H$，从而 $ha\in Ha=aH$. 故存在 $h_1\in H$ 使 $ha=ah_1$，从而 $a^{-1}ha=h_1\in H$，故 $a^{-1}Ha\subseteq H$.

$\Leftarrow$ 设 $ah\in aH$，则 $h\in H$，从而 $(a^{-1})^{-1}h(a^{-1})\in H$，故存在 $h_1\in H$ 使 $aha^{-1}=h_1$，故 $ah=h_1a\in Ha$，从而 $aH\subseteq Ha$，又 $a^{-1}ha\in a^{-1}Ha\subseteq H$，从而存在 $h_2\in H$，使 $a^{-1}ha=h_2$，故 $ha=ah_2\in aH$，从而 $Ha\subseteq aH$.

综上所述 $Ha=aH$.

定理 2.3.7　令 φ 是群 G 到群 H 的同态，则有：

1) $\mathrm{Im}\varphi$ 是群 H 的子群；

2) $\mathrm{Ker}\varphi$ 是群 G 的正规子群.

证明　1) 任取 $h_1,h_2\in\mathrm{Im}\varphi=\{\varphi(g),g\in G\}$，则依集 $\mathrm{Im}\varphi$ 的定义，必有 $g_1,g_2\in G$，使得

$$h_1=\varphi(g_1),h_2=\varphi(g_2).$$

这时

$$h_1h_2=\varphi(g_1)\varphi(g_2)=\varphi(g_1g_2)\in\mathrm{Im}\varphi,$$

$$h_1^{-1}=\varphi(g_1)^{-1}=\varphi(g_1^{-1})\in\mathrm{Im}\varphi,$$

即集 $\mathrm{Im}\varphi$ 是 H 的子群.

2) 任取 $g_1,g_2\in\mathrm{Ker}\varphi=\{g\in G\mid\varphi(g)=e\}$，则

$$\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)=ee=e,$$

$$\varphi(g_1^{-1})=\varphi(g_1)^{-1}=e^{-1}=e,$$

$$\varphi(ag_1a^{-1})=\varphi(a)\varphi(g_1)\varphi(a^{-1})=\varphi(a)e\varphi(a)^{-1}=e,$$

即得 $\mathrm{Ker}\varphi$ 是群 G 的正规子群.

定理 2.3.8（群的第一同态定理）　1) 若群 H 是群 G 的正规子群，则

$$\varphi: G \to G/H$$
$$g \mapsto gH$$

是群 G 到其商群 G/H 的满同态；

2)设 φ 是群 G 到群 $\overline{G}=\mathrm{Im}\varphi$ 的满同态，而 $H=\mathrm{Ker}\varphi$，则 $G/H\cong\overline{G}$.

证明　1)$\varphi: G\to G/H=\{aH \mid a\in G\}, g\mapsto gH$. φ 是一个满射；另一方面

$$\varphi(a)\times\varphi(b)=aH\times bH=abH, \varphi(ab)=abH,$$

即 φ 保持运算：

$$\varphi(ab)=\varphi(a)\times\varphi(b),$$

故 φ 是 G 到商群 G/H 的同态.

2)令 $H=\mathrm{Ker}\varphi$，H 是 G 的正规子群，商群 $G/H=\{gH, g\in G\}$，令

$$\theta: G/H\to\overline{G},$$
$$gH\mapsto\varphi(g).$$

验证 θ 是集 G/H 到 $\overline{G}$ 的一个映射：若 $gH=g'H$，$g,g'\in G$，必有 $\varphi(g)=\varphi(g')$，即 gH 的象与 gH 的代表元素 g 的选择无关. 由于 $g'\in gH$，故存在 $h\in H$，$g'=gh$，这样

$$\varphi(g')=\varphi(gh)=\varphi(g)\varphi(h)=\varphi(g)e=\varphi(g).$$

再证 θ 是单的，即要证：若 $\varphi(g_1)=\varphi(g_2)$，则 $g_1H=g_2H$. 由于

$$\varphi(g_1^{-1}g_2)=\varphi(g_1^{-1})\varphi(g_2)=\varphi(g_1)^{-1}\varphi(g_2)=\varphi(g_1)^{-1}\varphi(g_1)=e,$$

故 $g_1^{-1}g_2\in\mathrm{Ker}\varphi=H$，而有 $g_2\in g_1H$，即 $g_2H=g_1H$.

最后由于 φ 是满射，$\mathrm{Im}\varphi=\{\varphi(g), g\in G\}=\overline{G}$，而由 θ 之定义知 $\mathrm{Im}\theta$ 也等于 $\{\varphi(g), g\in G\}$，故 θ 是满射.

至此证得 θ 是 G/H 到 $\overline{G}$ 上的一一对应，且 θ 保持运算：

$$\theta(g_1H\cdot g_2H)=\theta(g_1g_2H)=\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)=\theta(g_1H)\cdot\theta(g_2H).$$

群 G 的同态像 $\overline{G}$ 可设想为群 G 的一个“粗略”的模型：忽略了 G 中某些元素间的差异而又维持 G 中的运算关系. 上述定理说，群 G 的所有可能的“粗略”模型就是群 G 的那些商群.

保持运算的同态映射当然把群 G 中所有运算关系（指涉及元素和运算的所有等式）都传递给 G 的同态像 $\overline{G}$，所以 $\overline{G}$ 保持着 G 中的某些结构. 例如，若 G 是交换群，则 $\overline{G}$ 也是；若在 G 中的所有元素的阶都小于 n，则在 $\overline{G}$ 中所有元素的阶也都小于 n. 反过来当然不对，有时 $\overline{G}$ 交换，而 G 是非交换. 下面定理说明子群与它商群的子群之间的关系.

定理 2.3.9（群的第二同态定理）　设 φ 是群 G 到群 $\overline{G}$ 上的满同态，$H=\mathrm{Ker}\varphi$. 令 $L(G,H)=\{G$ 中所有包含 H 的子群$\}$，$L(\overline{G})=\{\overline{G}$ 中所有子群$\}$，则

$$\theta:\ L(G,H)\rightarrow L(\overline{G})$$

$$S\longmapsto\varphi(S)=\{\varphi(s),s\in S\}=\overline{S}$$

是集 $L(G,H)$ 到集 $L(\overline{G})$ 上的一个一一对应，且有

(1) $S\supseteq T$ 当且仅当 $\varphi(S)\supseteq\varphi(T)$；

(2) S 是 G 的正规子群当且仅当 $\varphi(S)$ 是 $\overline{G}$ 的正规子群；

(3) 当 S 是 G 的正规子群时，有 $G/S\cong\overline{G}/\varphi(S)$.

问题 2.3

1. 利用 § 1.4 给出的三判据，对 C_{3v} 和 C_{4v} 的群元进行共轭分类.

2. 对 C_{3v} 群相应子群 (E,m_a) 完成陪集分解. $H=(E,m_a)$ 是正规子群吗？

3. C_{3v} 的子群 $H=(E,C_3^1,C_3^2)$ 是正规子群吗？求其商群 $K=C_{3v}/H$.

4. 试由生成元 C_4^1,σ_μ 生成群 C_{4v} 所有的群元.

5. 试证相位因子集合 $e^{i\theta}$，其中 θ 为实参数，相对于普通复数乘法，构成一连续群. 请找出该群的生成元，并说明全部群元如何生成.

6. 验证矩阵集合在矩阵乘法下构成群，给出相应群表，找到此群的一个正规子群，并据此求商群.

7. 设 G 为群，$G'<H\leqslant G$，证明：$H\lhd G$.

8. G 为如下集合：

$$\left\{\begin{pmatrix}\omega^k & 0\\ 0 & \omega^{-k}\end{pmatrix},\begin{pmatrix}0 & \omega^k\\ \omega^{-k} & 0\end{pmatrix}\middle|\ \omega=\cos\frac{2k\pi}{n}+\sin\frac{2k\pi}{n},k=0,1,\cdots,n-1\right\}$$

验证 G 对矩阵乘法成群，且 $G\cong D_n$，其中 D_{2n} 为二面体群.

9. 设 $\mathbf{Q}$ 是有理数加群，$\mathbf{Z}$ 是整数加群，证明：

(1)对于 $\mathbf{Q}$ 的一个非零数 $k,q\longmapsto kq$ 是 $\mathbf{Q}$ 到 $\mathbf{Q}$ 的自同构；

(2)$\mathbf{Q}$ 没有有限指数的真子群，由此 $\mathbf{Q}/\mathbf{Z}$ 没有有限指数的真子群；

(3)$\mathbf{Q}$ 没有极大子群.

10. 设 G 是交换群，且 $|G|=p_1\cdots p_r$，其中 $p_1,\cdots,p_r$ 是两两不同的素数，证明 G 是循环群.

11. 设 H 是 G 的真子群，证明 $G\neq gHg^{-1}$.

12. 设 H 是群 G 的子群，记 $M=\{Hg\,|\,g\in G\}$ 和 $T(M)$ 是 M 上全体变换在合成下形成的群(此时记变换的作用在右边). 对$\forall\ x\in G$，定义：

$$f_x:M\rightarrow M,Hg\longmapsto Hgx,$$

求证：1)对$\forall\ a,b\in G$，f_a 是 M 上的一个变换，且 $f_af_b=f_{ab}$；

2)如果定义 $\varphi:G\rightarrow T(M)$，$a\longmapsto f_a$，那么 φ 是群同态，且 $\mathrm{Ker}\varphi=\bigcap_{g\in G}g^{-1}Hg$.

§2.4　群的置换表示理论初步

我们说过同态是研究群之间关系的基本手段. 为了研究一个群 G，自然希望有一些理想的“样板”群作为标准，然后通过研究 G 到样板群的各种同态来把握 G 的特性. 理想的样板群有两类，一类是置换群，另一类是矩阵群. 一个群 G 到置换群的同态叫 G 的置换表示，而到矩阵群的同态叫线性表示.

研究群的线性表示是群论的一个美妙的分支，即通常所谓群表示理论，它在物理、化学、力学等许多方面都得到重要应用.

本节的目的是介绍群的置换表示理论的一些基本知识.

定义 2.4.1　设 Σ 是一个集合，$S(\Sigma)$ 是 Σ 上的对称群，群 G 到 $S(\Sigma)$ 的每个同态 $f: G\to S(\Sigma)$ 都叫做群 G 在集合 Σ 上的一个置换表示.

如果 f 是单同态，则称 f 是忠实表示.

这时，对于 G 中不同的元素 g，$f(g)$ 是 Σ 上不同的置换. 群 G 借助于置换表示 f 作用在集合 Σ 之上，也就是说，元素 $g\in G$ 在集合 Σ 上的作用看成是置换 $f(g)$，对于每个 $a\in\Sigma$，定义 $ga=f(g)a$.

设 $\pi: G\to S(\Sigma)$ 是一个置换表示. 在 Σ 上定义如下的关系：对于 $a,b\in\Sigma$，$a\sim b\Leftrightarrow$ 有 $g\in G$，使得 $ga=b$. 这是一个等价关系，因为

(1) $\pi(1_G)$ 是 Σ 的恒等置换，从而对每个 $a\in\Sigma$，$1_G\cdot a=a$，即 $a\sim a$；

(2) 如果 $a\sim b$，则有 $g\in G$ 使得 $ga=b$，于是 $g^{-1}b=a$，即 $b\sim a$；

(3) 若 $a\sim b$，$b\sim c$，则 $ga=b$，$hb=c$，其中 $g,h\in G$，于是 $(hg)a=c$，即 $a\sim c$. (简言之，$\sim$ 是等价关系，因为 G 是群)

定义 2.4.2　对上述等价关系，Σ 中元素 a 所在的等价类 $[a]=Ga=\{ga\mid g\in G\}$ 每个等价类叫一个 G-轨道，或简称轨道.

于是 Σ 分拆成一些轨道，在同一轨道中，可以通过某个 $g\in G$ 的作用将其一个元变为另一个元，而不同轨道中的两个元不可以这样做.

定义 2.4.3　如果 G 在 Σ 上的作用只有一个轨道，则称 G 在 Σ 上是传递的.

如果将 G 看成它在某一个 G-轨道上的作用，则 G 显然是传递的.

例 2.4.1　设 G 是群，取 $\Sigma=G$ 作如下映射：$f: G—S(G)$，$f(g)a=ga$，

对每个 g、$a\in G$. 也就是说，对于 $g\in G$，$f(g)$ 是集合 G 上如下的置换：它将 G 的每个元素 a 变成 ga(由群 G 上的消去律可知 $f(g)$ 是 G 上的置换). 由于

$$(f(g)f(g'))a=f(g)(f(g')a)=f(g)(g'a)=gg'a=f(gg')a,$$

从而 $f(g)f(g')=f(gg')$，即 $f: G\to S(G)$ 是群的同态.

定义 2.4.4 f 是群 G 在集合 G 上的一个置换表示，这叫做群 G 的左正则表示. 由于 $g\in \mathrm{Ker}f \Leftrightarrow ga=a, \forall a\in G \Leftrightarrow g=1_G$. 于是 f 为单同态，即左正则表示是忠实的. 类似地定义：

$$\tau: G\to S(G), \tau(g)=ag^{-1},$$

$$\tau(g)\tau(g')a=\tau(g)ag'^{-1}=ag'^{-1}g^{-1}=a(gg')^{-1}=\tau(gg')a,$$

可知 τ 也是一个群同态. 表示 τ 叫做 G 的右正则表示，它也是忠实的.

定理 2.4.1(Cayley 定理) 每个群均同构于某个置换群.

证明 由于正则表示 f(或者 τ)：$G\to S(G)$ 是忠实的，根据同态基本定理，G 同构于 $f(G)$，而 $f(G)$ 是集合 G 上对称群 $S(G)$ 的子群，从而 $f(G)$ 是集合 G 上的置换群.

这个定理充分显示出置换群可以作为一切群的样板群. 但是一般来讲，集合 G 太大，我们希望能给出群 G 在较小集合 Σ 上的置换表示，因为一般来说，$n=|\Sigma|$ 愈小，$S(\Sigma)=S_n$ 的子群愈容易研究.

例 2.4.2 设 $H\leqslant G$. 取 $\Sigma=\{aH|a\in G\}$，即 Σ 是 G 对于 H 的全部陪集 aH 构成的集合，定义 $f_H: G\to \mathbf{S}(\Sigma), f_H(g)(Ah)=gaH$，即对每个 $g\in G$，$f_H(g)$ 把陪集 aH 变成 gaH，这是集合 Σ 上的置换，并且 f_H 是群的同态，从而 f_H 给出的一个 G 置换表示，叫做 G 对于 H 的左诱导表示. 由于

$$g\in \mathrm{Ker}f_H \Leftrightarrow gaH=aH, \forall a\in G \Leftrightarrow a^{-1}ga\in H, \forall a\in G$$

$$\Leftrightarrow g\in aHa^{-1}, \forall a\in G \Leftrightarrow g\in \bigcap_{a\in G} aHa^{-1}.$$

从而 $\mathrm{Ker}f_H=\bigcap\limits_{a\in G} aHa^{-1}=H$ 的所有共轭子群的交.

类似可定义 G 对于子群 H 的右诱导表示：

$$\Sigma=\{Ha|a\in G\}, \quad \tau_H: G\to S(\Sigma), \quad \tau_H(g)(Ha)=Hag^{-1}.$$

$\mathrm{Ker}\tau_H$ 也是 H 的所有共轭子群的交.

例 2.4.3 设 A 是群 G 的任意子集，$\Sigma=\{aAa^{-1}|a\in G\}$，定义

$$\pi: G\to S(\Sigma), \pi(g)(aAa^{-1})=ga\ Aa^{-1}g^{-1}=(ga)A(ga)^{-1},$$

这是一个置换表示，叫做群 G 对于子集 A 的共轭表示. 由于

$$g\in \mathrm{Ker}\pi \Leftrightarrow gaAa^{-1}g^{-1}=aAa^{-1},$$

$$\forall a\in G \Leftrightarrow a^{-1}ga\in N_G(A); \forall a\in G \Leftrightarrow g\in aN_G(A)a^{-1}, \forall a\in G.$$

从而 $\mathrm{Ker}\pi=\bigcap\limits_{a\in G} aN_G(A)a^{-1}$ 为正规化子 $N_G(A)$ 的所有共轭子群的交.

定义 2.4.5 设群 G 作用于集合 Σ 之上，则对每个元素 $a\in\Sigma$，$G_a=\{g\in G|ga=a\}$ 是 G 的一个子群，叫做元素 a 的固定子群.

定理 2.4.2 设有限群 G 作用于集合 Σ 上 $a\in\Sigma$，则 $|G|=|G_a||[a]|$.

证明 作 G 对子群 G_a 的陪集分解

$$G=g_1G_a\cup g_2G_a\cup\cdots\cup g_nG_a, n=[G:G_a]$$

令 $g_ia=a_i$，$1\leqslant i\leqslant n$，对每个 $g\in G$，则有唯一 $i(1\leqslant i\leqslant n)$ 使得 $g\in g_iG_a$，令 $g=g_ih$，$h\in G_a$，则 $ga=g_iha=a_i$. 但是

$$a_i=a_j\Leftrightarrow g_ia=g_ja\Leftrightarrow g_j^{-1}g_ia=a\Leftrightarrow g_j^{-1}g_i\in G_a\Leftrightarrow g_iG_a=g_jG_a\Leftrightarrow i=j,$$

从而 $a_1,a_2,\cdots,a_n$ 互异，$[a]=\{a_1,a_2,\cdots,a_n\}$ 是 n 元的集合，即 $|[a]|=n=[G:G_a]=|G|/|G_a|$.

注意：(1)当 G 是无限群时，如果$[G:G_a]$有限，则 $|[a]|=[G:G_a]$也是正确的.

(2)利用例 2.4.3 的共轭表示和定理 2.4.2，我们重新得到前面所证的：设 A 为群 G 的子集，则 A 的共轭子集个数等于$[G:N_G(A)]$.

例 2.4.4　正 n 边形的对称群$(n\geqslant 3)$.

设正 n 边形的顶点依次为 $1,2,\cdots,n$，通过平面上欧氏运动和反转将正 n 边形变成自身的每个运动叫做该正 n 边形的一个对称. 全体这种对称自然形成一个群，叫做正 n 边形的对称群，记成 D_n.

D_n 中的元素显然是正 n 边形，2 个顶点的一个置换，并且它由这个置换完全决定，所以我们可以把 D_n 看成是 n 个顶点$\{1,2,\cdots,n\}$上的置换群. 首先，绕正 n 边形中心 O 反时针旋转 $2\pi/n$ 角度是 D_n 中的元素，它看成顶点置换则为 $\sigma=(1\ 2\ 3\ \cdots n)$，这是 n 阶元素.

由于 $\sigma^i(1)=i+1(0\leqslant i\leqslant n-1)$，所以 D_n 在$\{1,2,\cdots,n\}$上的作用是传递的. 其次，将顶点 1 固定的对称一共有两个，除了恒等置换之外还有将顶点 1 保持不动的反射，若 2 整除 n，则

$$\tau=(2,n)(3,n-1)\cdots(n/2,n/2+2);$$

若 2 不整除 n，则

$$\tau=(2,n)(3,n-1)\cdots((n+1)/2,(n+3)/2).$$

从而顶点 1 的固定子群是 2 阶的. 根据轨道公式便知 $|D_n|=2n$.

注意 τ 是 2 阶的元素. $\sigma^i\tau^j(0\leqslant i\leqslant n-1,0\leqslant j\leqslant 1)$是 $2n$ 个不同的对称，它们给出群 D_n 的全部元素. 这个群的运算法则由 $\sigma^n=^1,\tau^2=1$ 和 $\tau\sigma=\sigma^{-1}\tau$ 完全决定.

引理 2.4.3　设 G 是 $2n$ 阶群，2 不整除 n，则 G 必有指数为 2 的正规子群.

证明　考虑 G 的左正则表示 $f:G\text{—}S(G)=S_{2n}$，由于 f 是忠实表示，$G\cong f(G)$，因此只须对置换群 $f(G)$证明引理. 注意群 G 中必有 2 阶元素 $g,g\neq 1,g^2=1$，由于 $f(g)a\neq a$，$f(g)^2a=a$，$\forall\ a\in G$，置换 $f(g)$是一些对换$(a,f(g)a)$之积. G 共有 $2n$ 个元素，从而 $f(g)$是 n 个对换之积. 由假设 n 是奇数，$f(g)$为奇置换. 我们证明了群 $f(G)$中含有奇置换，从而 $f(G)$中的偶置换成了 $f(G)$的指数为 2 的子群，指数为 2 的子群必是正规的.

定理 2.4.4　G 为有限群，$|G|\geqslant 6$ 且 $|G|\equiv 2(\mathrm{mod}4)$，则 G 不是单群.

引理 2.4.5　设 G 为有限群，p 是 $|G|$ 的最小素因子，如果 $N\leqslant G$，$[G:N]=p$，则 N 是 G 的正规子群.

证明　考虑 G 对于子群的诱导表示：

$$f: G\to S_p, \mathrm{Ker}f=\bigcap_{a\in G}a^{-1}Na\leqslant N,$$

从而 $p=|G|/|N|$ 除尽 $|G|/|\mathrm{Ker}f_N|$. 由于 p^2 不整除 $p!=|S_p|$，而 $G/\mathrm{Ker}f_N$ 同构于 S_p 的一个子群，因此 p^2 除不尽 $|G/\mathrm{Ker}f_N|$.

另一方面，$|G/\mathrm{Ker}f_N|$ 没有比 p 大的素因子，由对 p 的假设它也没有比 p 小的素因子，从而 $|G/\mathrm{Ker}f_N|=p$，但是 $[G:N]=p$ 且 $\mathrm{Ker}f_N\leqslant N$，因此 $N=\mathrm{Ker}f_N$，于是 N 是 G 的正规子群.

问题 2.4

1. 设 G 作用在集合 Σ 上，$\forall\, a,b\in\Sigma$，若存在 $g\in G$ 使得 $ga=b$，则 $G_a=g^{-1}G_bg$. 换句话说，同一轨道中元素的固定子群彼此共轭.

2. 求正四面体、正立方体、正八面体、正十二面体和正二十面体的对称群各有多少元素？这五个对称群当中是否有同构的？

3. 设群 G 在集合 Σ 上的作用是传递的，N 是 G 的正规子群，则 Σ 在 N 作用下的每个轨道有同样多的元素.

4. 设群 G 作用在集合 Σ 上. 令 t 表示 Σ 在 G 作用下的轨道个数，对任意 $g\in G$，$f(g)$ 表示 Σ 在 g 作用下的不动点个数. 试证：$\sum\limits_{g\in G}f(g)=t|G|$.

这就是说，G 的每个元素在 Σ 上作用平均使 t 个文字不动.

5. 设 p 是一个素数，G 是 p 的方幂阶的群. 试证：G 的非正规子群的个数一定是 p 的倍数.

6. 令 G 是单群，如果存在 G 的真子群 H 使得 $|G:H|\leqslant 4$，则 $|G|\leqslant 3$.

7. 试证：全线性群 $GL(n,C)$ 不含有指数有限的真子群.

8. 令 G 是阶数为 2^nm 的群，其中 m 是奇数. 如果 G 含有一个 2^n 阶的元素，则 G 含有一个指数为 2^n 的正规子群.

9. 设 a 是有限群 G 的一个自同构. 若对任意 $g\in G$，g 和 $a(g)$ 共轭，则 a 的阶的每个素因子都是 $|G|$ 的因子.

10. 设 p 是 $|G|$ 的最小素因子，p 阶子群 A 是 G 的正规子群，则 $A\leqslant C(G)$.

11. 证明：阶为不小于 $r!$ 的有限单群没有指数为 r 的子群.

12. 证明：群 G 双传递地作用在集 X 上$\Leftrightarrow G$ 传递的作用在 $X-\{x\}$，$x\in G$.

13. 证明：对群 G 中任意的元素 $g,x,C_G(gxg^{-1})=gC_G(x)g^{-1}$成立.

14. 设 G 为有限群，求证：$|\{(a,b)\in G\times G|ab=ba\}|=r|G|$，其中 r 为 G 的共轭类的个数.

Galois 小传

伽罗瓦(Galois)，法国数学家，1811 年 10 月 25 日生于巴黎近郊布拉伦. Galois 幼年受到良好的家庭教育，12 岁进入巴黎一所公立中学，1827 年开始自学勒让德、拉格朗日、高斯和柯西等大师的经典著作和论文. 18 岁时，他完成了一篇代数方程理论方面的重要论文，并递交给了法国科学院请求发表. 论文交由柯西审阅，柯西给予了肯定，但随后就石沉大海. 以后他投到巴黎科学院的论文又有两次被遗失或退回. 在 1828 年至 1830 年，他得到了后来被称为"Galois 理论"的重要结论.

1830 年 Galois 进入巴黎高等师范学校学习，由于参加政治斗争，公开反对国王制度，被学校除名，并两次入狱. 1832 年 5 月 30 日，Galois 由于政治和爱情的纠葛在决斗中被人射中，第二天就不幸去世，死时还不满 21 岁. 在 Galois 之前，数学家们已经找到了一至四次代数方程的求根公式，而用根式求解一般的五次方程是不可能的这一结论直到 1824 年 Abel 才给出了一个基本正确的证明. Galois 并不知道 Abel 的工作，他深入研究了方程能用根式求解的必须满足的本质条件，建立了方程与由方程的根所定义的扩域以及根的"容许"置换组成的群之间的关系. 他得到了代数方程能用根式解的充要条件是它所对应的群可解，由此，他认识到五次及五次以上的方程需要用完全不同于低次方程的方法. 他提出的"Galois 域"、"Galois 群"和"Galois 理论"是近世代数所研究的重要课题.

Galois 的工作成果是 19 世纪数学中最杰出的成就之一. Galois 理论是代数学发展中的一个里程碑. Galois 之前，代数学研究的中心问题是代数方程的求根问题，而 Galois 之后，代数学的中心问题渐渐转移到研究群、环、域等代数系统的结构与分类，步入了近世代数的阶段.

Galois 生前并未获得应有的荣誉. 在决斗前夕，他给好友写了封信，请求把他的论文公诸于世，但并没有引起人们的注意. 直到 1846 年，他的附有刘维尔注释的手稿才在《纯粹和应用数学杂志》上发表. 1870 年，法国数学家若尔当在其著作《置换和代数方程论》中对 Galois 理论作了长篇论述. 从此，Galois 的工作才被完全理解，同时也确立了他在数学史上的地位.

§ 2.5　有限群的 Sylow 定理

拉格朗日定理指出：若有限群 G 的阶数是 n，则 G 的每个子群的阶都是 n 的因子. 反过来，对于 n 的每个因子 d，G 未必有 d 阶子群. 例如我们已知 60 阶群 A_5 是单群，它没有 30 阶子群，因为这样的子群一定是正规的. 但是下一定理表明，对于 $|G|$ 的特殊的因子 d，G 必有 d 阶子群. 在本定理以及以后许多结果的证明中，我们不断使用群在集合上的作用这一有效工具.

定理 2.5.1　设 $p^r \mid |G|$，其中 p 为素数，以 $N(n)$ 表示 G 中 n 阶子群的个数，则 $N(p^r) \equiv l(\mathrm{mod}\, p)$. 特别地，如果 $p^r \mid |G|$，则 G 至少存在一个 p^r 阶子群.

证明　令 $|G| = p^r n$，以 Σ 表示 G 的全部 p^r 元子集组成的集族，则 $|\Sigma| = C_{np^r}^{p^r}$，考虑 G 在 Σ 上的如下作用

$$f: G \to S(\Sigma),\ f(g)M = Mg^{-1},\ \forall\ g \in G, M \in \Sigma.$$

Σ 分拆成一些轨道 T_i 之并 $\Sigma = \bigcup_i T_i$，$|\Sigma| = \Sigma_i |T_i|$，$|T_i| = |G : A_i|$，其中 $A_i = g \in G \mid M_i g^{-1} = M_i\}$ 是轨道 T_i 中任一元素 M_i 的固定子群，由于 $M_i A_i = M_i$，M_i 可以分拆成 $M_i = \bigcup_{j=1}^{k_i} g_{ij} A_i$，$g_{ij} \in M_i$，$1 \leqslant j \leqslant k_i$，$k_i = |M_i| / |A_i| = p^r / |A_i|$.

于是 $|A_i| = p^{r_i}$，$r_i \leqslant r$，如果 $r_i < r$，则 $|T_i| = [G : A_i] = np^{r-r_i} \equiv 0(\mathrm{mod}\, pn)$. 若 $r_i = r$，则 $|T_i| = n$. 于是 $C_{np^r}^{p^r} = |\Sigma| = \Sigma_i |T_i| \equiv \Sigma_{|T_i|=n} |T_i| = n = n\Sigma_{|T_i|}, 1(\mathrm{mod}\, pn)$.

现在计算 $\sum\limits_{|T_i|=n} 1$，即长为 n 的轨道 T_i 的个数，注意

$$|T_i| = n \Rightarrow |A_i| = p^r \Rightarrow k_i = 1 \Rightarrow M_i = g_i A_i,$$

于是 p^r 阶子群 $B_i = g_i A_i g_i^{-1}$ 与 $M_i = g_i A_i$ 在同一轨道 T_i 之中，并且若 $X \in T_i$，则 $Xg = M_i = B_i g_i$，$X = B_i g_i g^{-1}$，所以轨道 T_i 中 n 个元素即是 G 对于 p^r 阶子群 B_i 的 n 个陪集. 注意这 n 个陪集中除 B_i 外其余陪集不包含 1，从而不会是子群. 这表明，G 的每个 p^r 阶子群均恰好在一个长为 n 的轨道之中，于是 $\sum\limits_{|T_i|=n} 1 = N(p^r)$，从而 $C_{np^r}^{p^r} \equiv nN(p^r)(\mathrm{mod}\, pn)$. 这个同余式对任意 $p^r n$ 阶群 G 均成立，特别是 G 为循环群，则它只有一个 p^r 子群，代入上式 $C_{np^r}^{p^r} \equiv n(\mathrm{mod}\, pn)$. 于是 $n \equiv nN(p^r)(\mathrm{mod}\, pn)$，从而 $N(p^r) \equiv 1(\mathrm{mod}\, p)$.

定义 2.5.1　设 G 为 $p^r n$ 阶群，其中 p 为素数，$r \geqslant l$，p 不整除 n，则 G 的每个 p^r 阶子群均叫做 G 的 Sylow$p$-子群.

定理 2.5.2(Sylow 定理)　设 G 为有限群，则

(1)对 $|G|$ 的每个素因子 p，均存在 G 的 Sylow$p$-子群；

(2)G 的 Sylow$p$-子群彼此共轭；

(3)G 的 Sylow$p$-子群的个数$\equiv 1 (\bmod p)$；

(4)设 P 为 G 的一个 Sylow$p$-子群，则 Sylow$p$-子群的个数为$[G : N_G(P)]$.

证明　(1)和(3)由定理 2.5.1 直接推出，由(2)容易得到(4)，从而只需证(2). 令 Σ 是 G 的所有 Sylow$p$-子群构成的集合，将 G 共轭作用于其上. 令 Δ 是一个 G-轨道. 取 $P \in \Sigma$，再将 P 共轭作用于 Δ 上. Δ 分拆成一些 P-轨道，每个 P-轨道的长度是 $|P| = p^r$ 的因子.

如 $P \in \Delta$，并且 P' 自身组成一个 P-轨道，即 $Xp'x^{-1} = P'$，$\forall\ x \in P$，则 $P \leqslant N_G(P')$，从而 $PP' \leqslant G$，但是 $|P\ P'| = |P||P'|/|P \cap P'|$ 仍为 P 的幂，且 $P \leqslant PP'$，由于 P 和 P' 均是 Sylow$p$-子群. 故必 $P' = PP' = P$. 这就表明当 $P \in \Delta$ 时，Δ 中长为 1 的轨道只有 $\{P\}$，从而 $|\Delta| \equiv 1 (\bmod p)$. 当 $P \notin \Delta$ 时，Δ 没有长为 1 的轨道，从而 $|\Delta| \equiv 0 (\bmod p)$.

这两种情形不可能同时发生，所以只能是所有 Sylow$p$-子群均在 Δ 中，即 $\Sigma = \Delta$，换句话说，G 在 Σ 上的共轭作用是传递的，即 G 的所有 Sylow$p$-子群彼此共轭.

推论 2.5.3　设素数 p 是 $|G|$ 的因子，则群 G 的每个 p 方幂阶的子群 B 均包含在 G 的某个 Sylow$p$-子群内.

证明　仍以 Σ 表示 G 的全部 Sylow$p$-子群，则 $|\Sigma| \equiv 1 (\bmod p)$. 将 B 共轭作用在 Σ 上，每个 B-轨道的长度是 $|B|$ 的因子，从而为 p 的方幂，由 $|\Sigma| \equiv 1 (\bmod p)$ 可知必有长为 1 的 B-轨道$\{P\}$. 与证明定理 2 的(2)一样可由此推出 $BP = P$，于是 $B \leqslant P$，即 B 包含在 Sylow$p$-子群 P 内.

推论 2.5.4　设 P 是 G 的 Sylow$p$-子群，$A \leqslant G$，且 $N_G(P) \leqslant A$，则 $N_G(A) = A$.

证明　设 $g \in N_G(A)$，则 $g^{-1}Ag = A$，从而 $g^{-1}Pg \leqslant g^{-1}Ag = A$，由于 $P \leqslant N_G(A) \leqslant A \leqslant G$，则 P 为 A 的 Sylow$p$-子群，又 $g^{-1}Pg \leqslant A$，$|P| = |g^{-1}Pg|$，知 $g^{-1}Pg$ 也是 A 的 Sylow$p$-子群，存在 $a \in A$，使得 $a^{-1}(g^{-1}Pg)a = P$，即 $ga \in N_G(P) \leqslant A$，于是 $g \in A$.

推论 2.5.5　(弗拉梯尼(Fratini))　M 是 G 的正规子群，P 为 M 的 Sylow$p$-子群，则 $G = MN_G(P)$.

证明　对于 $\forall\ g \in G$，$g^{-1}Pg \leqslant g^{-1}Mg = M$. 由定理 2.7.2 知存在 $k \in M$，使得 $k^{-1}(g^{-1}Pg)k = P$，即 $gk \in N_G(P)$，从而 $g = (gk)k^{-1} \in N_G(P)M = MN_G(P)$.

例 2.5.1　148 阶群不是单群.

证明　取 $p = 37 | 148$，则 $N(37) \equiv 1 (\bmod 37)$，从而 $N(37) = 37l + 1$，由于 148 阶群 G 的全部 Sylow$p$-子群形成一个共轭类，其总数应当是 $|G| = 148$ 的因子，即 $N(37) = 37l + 1 | 148$. 于是 $37l + 1 | 4$，这只能 $l = 0$，即 $N(37) = 1$，因此 G 只有一个 37 阶子群必然是正规子群，G 不是单群.

例 2.5.2　56 阶群 G 不是单群.

证明　与前例一样，$N(7) = 7n + 1 | 56$，从而 $7n + 1 | 8$，于是 $N(7) = 1$ 或 8. 如果

$N(7)=1$，则 7 阶 Sylow-子群是正规的，如果 $N(7)=8$，令 $P_1,P_2,\cdots,P_8$ 是 G 的 8 个不同的 7 阶子群，它们中的任意两个只有公共元素 1_G，合起来共占了 $7\times8-7=49$ 个元素，余下 $56-49=7$ 个元素加上 1_G 必然形成 G 的 8 阶 Sylow$p$-子群，从而 G 的 Sylow$p$-子群只有一个，必为正规子群，G 不是单群.

定理 2.5.6 设 p 和 q 是两个素数，则 pq 阶群 G 不是单群.

证明 若 $p=q$，p^2 阶群 G 是 Abel 群，由定理 1 知它有 p 阶子群，Abel 群的子群都是正规的，所以 G 不是单群.

如果 $p\neq q$，不妨设 $p>q$，$N(p)=np+1\mid q$，而 $q<p$，只能，$n=0$. G 只有一个 Sylow$p$-子群，它是正规子群，于是 G 不是单群.

定理 2.5.7 设 p 和 q 是素数，则 p^2q 阶群 G 不是单群.

证明 若 $p=q$，已证过 p^3 阶群 G 必有非平凡的中心 $C(G)$，且 $C(G)$ 有 p 阶子群 N，显然 N 是 G 的正规子群，因此 G 不是单群.

如果 $p>q$，则 $N(p^2)=np+1\mid q$，$q<p$，于是 $n=0$. G 有正规的 p^2 阶 Sylow 子群，G 不是单群.

最后设 $p<q$，则 $N(q)=nq+1\mid p^2$. 如果 $N(q)=1$，则 G 有正规 q 阶子群，G 不是单群. 由于 $p<q$，$N(q)$ 不能为 p. 最后若 $N(q)=p^2$，即 G 有 p^2 个 q 阶子群，它们共占据 G 的 $p^2(q-1)+1$ 个元素，余下 p^2-1 个元素和 1_G 便构成 G 的唯一的 p^2 阶 Sylow 子群 P，P 是 G 的正规子群，所以 G 也不是单群.

定理 2.5.8 非 Abel 单群的最小阶数是 60，且它必同构于 A_5.

证明 到目前为止我们已证明了下列诸结果：

p^n($n\geqslant2$，p 为素数)阶群有非平凡中心，因此不是单群；

pq，p^2q(p 和 q 为素数)阶群均不是单群；

$2m$(m 为奇数，$m\geqslant3$)阶群不是单群.

在 59 之内除了上述情形后只剩下 $|G|=24,36,40,48,56$. 例 2.5.2 表明 56 阶群不单；40 阶群有唯一的 Sylow$p$-子群，也不是单群.

设 $|G|=48=3\times2^4$，易知 G 的 Sylow2-子群的个数为 1 或 3，若 $N(16)=1$，则 G 不单；若 $N(16)=3$，令 P_1,P_2,P_3 为 G 的 3 个 Sylow2-子群，G 在 $\{P_1,P_2,P_3\}$ 上的共轭作用给出同态 $f:G\to S_3$. 令 $N=\mathrm{Ker}f$，则 N 是 G 的正规子群. 由于 $|G|=48>|S_3|=6$，从而 $N\neq\{1\}$. 又由于 P_1,P_2,P_3 彼此共轭，$N\neq GL$，于是 N 是 G 的非平凡正规子群，因此 48 阶群不单. 类似地可证 24 阶群不单.

设 $|G|=36=2^2\times3^2$，则 G 的 Sylow3-子群的个数为 1 或 4，若 $N(9)=1$，则 G 不单. 若 $N(9)=4$，则 G 在 Sylow3-子群 $\{P_1,P_2,P_3,P_4\}$ 的集合上的共轭作用给出同态 $f:G\to S_4$. 由上面的方法断定 G 有非平凡正规子群，G 不是单群.

最后考虑$|G|=60$,已证过A_5为单群,现在我们证明60阶单群G必然同构于A_5.首先证明G有指数为5即12阶的子群.

为此,令P是G的一个4阶Sylow子群,$N(4)=[G:N_G(P)]$,由G为单群可知$N(4)\neq 1$,上面的方法同样给出$N(4)\neq 3$,从而$4\leqslant |N_G(P)|<15$.

由于$4\,|\,|N_G(P)|\,|\,60$,如果$|N_G(P)|\neq 12$,则必然$|N_G(P)|=4$,G有15个Sylow2-子群.如果它们两两只有公共元素1_G,则它们共占去G的$15\times 331=46$个元素,由于G为单群,G的Sylow5-子群至少有6个,它们有$6\times 4+1=25$个元素,上述所有子群的任意两个均只有公共元素1_G,从而总共有$46+25-1=70$个元素,但$|G|=60$,这一矛盾表明必有两个不同的Sylow2-子群P和P'存在,使得$P\cap P'=K\neq\{1\}$.由于P和P'都是Abel群,$\langle P,P'\rangle$是$C_G(K)$的子群.因为$P\neq P'$,P和P'生成的群$\langle P,P'\rangle$的阶大于4,于是$4<|C_G(K)|<15$.

但$4\,|\,|C_G(K)|\,|\,60$,只能$|C_G(K)|=12$,因此G必有12阶子群.

设N为G的12阶子群,G对于N的诱导表示产生同态$f:G\to S_5$,由于f是单同态,G同构于S_5的一个60阶子群M,M是S的非平凡正规子群,M必然为A_5,这就完成了定理的证明.

Sylow 小传

西罗(P. L. Sylow),挪威数学家,1832年12月12日生于挪威克里斯蒂安尼亚(现称奥斯陆).1850年在克里斯蒂安尼亚教会学校毕业,后进入克里斯蒂安尼亚大学学习,曾获得数学竞赛金牌.

1855年,Sylow成为一名中学教师.尽管教书的职业花费了他大量的时间,但Sylow还是挤出时间来研究Abel的论文.在1862—1863学年中Sylow得到了克里斯蒂安尼亚大学的临时职位,为学生讲授Gaiois理论和置换群.在他当年的学生中,有一位后来成为著名数学家、李代数和李群的创始人——李(S. Lie).从1873年至1881年,Sylow同Lie合作,编辑出版了Abel著作的新版本.1902年又与别人合作出版了Abel的通信集.Sylow最重要的成就——Sylow定理是他在1872年获得的.在得知了Sylow的结果后,若尔当称它是"置换群论中最基本的结论之一".这些定理以后成为研究群论特别是有限群论的重要工具.Sylow对于椭圆函数论也有贡献.1898年他从中学退休后,任克里斯蒂安尼亚大学教授,直至1918年9月7日去世.

问题 2.5

1.若p是$|G|$的素因子,则群G必有p阶元素.

2.设G是一个n阶群,p是n的一个素因子,试证:方程$x^p=1$在群G中解的个数

是 p 的倍数.

3. 证明:6 阶非交换群只有 S_3.

4. 试证:200 阶群 G 一定含有一个正规的 Sylow 子群.

5. 确定 S_4 的不同的 Sylow 子群的个数.

6. 确定 S_4 的自同构群 $\mathrm{Aut}S_4$.

7. 设 N 是有限群 G 的一个正规子群,如果 p 和 $|G/N|$ 互素,则 N 包含 G 的所有 Sylow$p$-子群.

8. 设 N 是有限群 G 的正规子群,P 是 G 的一个 Sylow$p$-子群,试证:

(1)$N\cap P$ 是 N 的 Sylow$p$-子群;

(2)PN/N 是 G/N 的 Sylow$p$-子群;

(3)$N_G(P)N/N\cong N_{G/N}(PN/N)$.

9. 令 $P_1,P_2,\cdots,P_N$ 是有限群 G 的全部 Sylow$p$-子群,如果$\forall\ i\neq j$,总有$[P_i:P_i\cap P_j]\geqslant p^r$,则 $N\equiv 1(\bmod p^r)$.

10. 令 G 是集合 Σ 上的置换群,P 是 G 的 Sylow$p$-子群,$a\in\Sigma$,如果 p^m 整除 $|Ga|$,则 p^m 整除 $|Pa|$.

11. 令 G 是集合 Σ 上的置换群. $\forall\ a\in\Sigma$,设 P 是固定子群 G_a 的 Sylow$p$-子群,Δ 是轨道 Ga 在 P 作用下的全部不动点的集合. 试证 $N_G(P)$在 Δ 上的作用是传递的.

12. 设 G 为有限群,$H,K\lhd G,G=HK,P\in \mathrm{Sylow}_p(G)$. 求证:存在 $U\in \mathrm{Sylow}_p(H),V\in \mathrm{Sylow}_p(K)$使得 $P=UV$.

13. 设 G 为有限群,证明:若 $P\in \mathrm{Sylow}_p(G)$,则 $N_G(N_G(P))=N_G(P)$.

§2.6　有限交换群的结构

本节我们将看到非常漂亮完整的有限交换群的结构定理,由此我们将具体地理解什么是群的结构理论.

本节中 G 表示 Abel 群,群的运算记作加法"+",简称 G 为加群.

在加群 G 中我们已经知道 $ng(g\in G,n\in\mathbf{Z})$的意义. 我们可以把它解释成 $\mathbf{Z}\times G$ 到 G 的一个运算 $\cdot$,即规定 $n\cdot g=ng$. 这个运算 $\cdot$ 显然满足下列性质:对$\forall\ g,h\in G,n,m\in\mathbf{Z}$,有

1)$n\cdot(g+h)=n\cdot g+n\cdot h$;

2)$(n+m)\cdot g=n\cdot g+m\cdot g$;

3)$(nm)\cdot g=n\cdot(m\cdot g)$;

4)$1\cdot g=g$.

这样，加群 G 就变成一个与数域 F 上向量空间 V 相类似的对象了，只不过在向量空间 V 中谈论线性和时其系数取自数域 F，而对加群 G 而言，线性和 $m_1g_1+\cdots+m_kg_k$ 系数只能取自整数环 $\mathbf{Z}$.

把加群 G 和向量空间 V 进行类比是很有好处的，例如向量空间 V 的基本概念，两个向量等价的概念等都可以平移到加群 G 上来.

设子集 $H=\{h_1,\cdots,h_s\}\subseteq G$，规定

$$\mathbf{Z}\cdot H=\{n_1\cdot h_1+\cdots+n_s\cdot h_s \mid n\in\mathbf{Z}, 1\leqslant i\leqslant s\}$$

有 $\mathbf{Z}\cdot H=\langle H\rangle$，即 $\mathbf{Z}\cdot H$ 就是 H 生成的子群. 且当 $H=\{g_1,\cdots,g_s\}$ 是 G 的生成元时，$G=\mathbf{Z}\cdot H=Z\cdot g_1+\cdots+Z\cdot g_s$.

下面的概念在结构理论中起重要作用.

定义 2.6.1　设 G 是加群，而 $H_i, 1\leqslant i\leqslant s$ 是 G 的子群，如果

1) $G=H_1+\cdots+H_s$，即每一个 g 可表示成 $h_1+\cdots+h_s, h_i\in H_i$；

2) 上面的表示方法是唯一的，即对 $\forall\ g\in G$，由

$$g=h_1+\cdots+h_s=h'_1+\cdots+h_s',$$

其中 $h_i, h_i'\in H_i$ 一定有 $h_i=h_i', i=1,2,\cdots,s$.

则称 G 是子群 $H_1,\cdots,H_s$ 的(内)直和，记为 $G=H_1\oplus H_2\oplus\cdots\oplus H_s$，也称 G 可以分解成 $H_1,\cdots,H_s$ 的直和.

显然，群的直和与向量空间的直和是很类似的概念.

下面是一些经常用到的事实：

引理 2.6.1　在加群 G 中，

1) 若元素 g 的阶为 s，而 $(s,t)=1$，则 tg 的阶亦为 s，且 $\langle g\rangle=\langle tg\rangle$；

2) 若元素 g 的阶为 s，而 $(s,t)=d$，则 tg 的阶为 s/d；

3) 若 $g_l+\cdots+g_m=0$ 且 g_i 的阶 s_i 两两互素，则每个 $g_i=0$.

证明　1) $s(tg)=t(sg)=t0=0$，若 $\forall\ k(tg)=0$，有 $s\mid kt$ 又 $(s,t)=1$，有 $s\mid k$，所以 tg 的阶亦为 s.

显然 $\langle tg\rangle\subseteq\langle g\rangle$，由 $(s,t)=1$，存在 $u,v\in\mathbf{Z}$，使得 $su+tv=1$，则

$$g=1g=(su+tv)g=u(sg)+v(tg)=v(tg),$$

说明 g 可以由 tg 表示，即 $\langle g\rangle\subseteq\langle tg\rangle$，所以 $\langle tg\rangle=\langle g\rangle$；

2) 证略；

3) 对 m 用归纳法，不妨设 $m>1$，则 $s_mg_1+\cdots+s_mg_{m-1}=0$，对任意 $1\leqslant i\leqslant m-1$，由 $(s_m,s_i)=1$ 和 1) 知 s_mg_i 的阶也是 s_i. 故由归纳假设知 $s_mg_i=0$，又由 $(s_m,s_i)=1$ 知 $g_i=0$，即 $g_1=g_2=\cdots=g_{m-1}=0$，从而也有 $g_m=0$.

定理 2.6.2　设 G 是有限加群，$|G|=n=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$，其中 p_i 是不同素数. 则

1) $G=H_1\oplus H_2\oplus\cdots\oplus H_t$，其中 H_i 是 p_i-群，$i=1,\cdots,t$；

2) 若 $G=H_1\oplus\cdots\oplus H_t=H'_1\oplus\cdots\oplus H'_t$，其中 H_i,H'_i 是 p_i-群，$i=1,\cdots,t$，则对 $\forall\, i$，有 $H_i=H'_i$.

证明 1) 对 $\forall\ 1\leqslant i\leqslant t$，令 $n_i=p_i^{m_i}$，$r_i=n/n_i$，$H_i=\{g\in G\,|\,g$ 的阶是 p_i 的幂$\}$，那么 $H_i=\{g\in G\,|\,n_ig=0\}$，则 H_i 是 G 的子群. 从而得

$$H_1+H_2+\cdots+H_t=\{h_1+\cdots+h_t\,|\,h_i\in H_i,i=1,\cdots,t\}$$

是 G 的子群，$\forall\ g\in G$，注意到 $r_1,r_2,\cdots,r_t$ 的最大公因子是 1，由高等代数知，存在整数 $u_1,\cdots,u_t$，使得 $\Sigma_i u_ir_i=1$，则 $g=(\Sigma_i u_ir_i)g=\Sigma_i u_ir_i$，由 G 的阶为 n 知 $ng=0$，故

$$n_i(u_ir_ig)=u_i(r_in_ig)=u_i(ng)=0,u_ir_ig\in H_i,i=1,2,\cdots,t,$$

故 $g\in H_1+H_2+\cdots+H_t$. 于是 $G=H_t+\cdots+H_t$，由定义知 H_i 是 p_i-群.

易知定义 2.8.1 中的 2) 等价于：若 $h_1+\cdots+h_t=0$，这里 $h_i\in H_i$，则必有 $h_i=0,i=1,2,\cdots,t$. 而这是成立的，又因为 h_i 的阶为 p_i 的幂，而它们是两两互素的，故

$$G=H_1\oplus H_2\oplus\cdots\oplus H_t.$$

以上命题把有限加群的研究归结为对有限 p-加群的研究.

设 G 为加群且 $|G|=n=p^m$，p 是素数，我们想更精细地分解它. 如果 $G=\langle g\rangle=\mathbf{Z}g$ 是循环群，则 G 不能再分解，因为若

$$G=\mathbf{Z}g_1\oplus\mathbf{Z}g_2,|Zg_1|=p^{m_1},|Zg_2|=p^{m_2},$$

其中 $m_1\leqslant m_2<m$，则 $p^{m_2}G=0$，这与 g 的阶是 p^m 相矛盾. 这样从直和的角度来看，循环 p-群是最基本的构件了，它相当于向量空间中的一维子空间. 因而最好的结果将是把 p-加群 G 表成循环群的直和.

假设我们有 $G=\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_k$，我们想知道 $\{g_1,\cdots,g_k\}$ 这个 G 的生成元集在 G 的所有生成元集中有一些什么特殊的地位和性质，从而能使我们利用它把这个特殊的生成元集找出来. 与向量空间的基相比较，容易想到这将是元数最小的生成元集，另一点将想到的是 g_i 的阶 p^{m_i} 组成的集合 $\{p^{m_1},\cdots,p^{m_k}\}$ 该有点什么"极端"的性质.

定义 2.6.2 设 $\{g_1,\cdots,g_k\}$，$\{h_1,\cdots,h_k\}$ 是 G 的两个元素个数相等的生成元集，其相应的阶集依次为

$$\{p^{m_1},\cdots,p^{m_k}\},\{p^{l_1},\cdots,p^{l_k}\},$$

如果 $m_1+\cdots+m_k<l_1+\cdots+l_k$，我们就说生成元集 $\{g_1,\cdots,g_k\}$ 小于生成元集 $\{h_1,\cdots,h_k\}$.

定理 2.6.3 G 为有限 p-加群，$|G|=p^m$，则有

1) $G=\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_k$；

2) 若 $G=\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_k=\mathbf{Z}h_1\oplus\cdots\oplus\mathbf{Z}h_s$，则必有 $k=s$，且适当重排脚标后有 $Zg_i\cong Zh_i,i=1,\cdots,k$.

证明 1)显然 G 有有限生成元集,因而有元素个数最小(设为 k)的生成元集,在这些元素个数最小的生成元集中,必有一按上面规定的大小关系是极小的生成元集,任取其中一个,记作 $\{g_1,\cdots,g_k\}$,其相应阶集为 $\{p^{r_1},\cdots,p^{r_k}\}$. 对生成元集而言,显然有 $G=\mathbf{Z}g_1+\cdots+\mathbf{Z}g_k$.

下面证 $G=\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_k$. 用反证法,若不然,则有(不妨设为三项)$i<j<t$,$l_ig_i+l_jg_j+l_tg_t=0$,它们都不等于 0,若 l_i 不被 p 整除,此时 l_i 和 g_i 的阶互素,则有

$$l_ig_i=-l_jg_j-l_tg_t,\mathbf{Z}g_i=\mathbf{Z}(l_ig_i)\subseteq\mathbf{Z}g_j+\mathbf{Z}g_t,$$

上式中第一个等号的根据是引理 2.8.1,这时从元数最小的生成元集 $\{g_1,\cdots,g_k\}$ 中去掉元素 g_i 后仍是生成元集,这是不可能的. 故不妨设 l_i,l_j,l_t 都被 p 整除,设 $(l_i,l_j,l_t)=p^sl$,其中 p 与 l 互素,$s\geqslant1$,则 1)可改写成 $p^s(m_ig_i+m_jg_j+m_tg_t)=0$,$m_i,m_j,m_t$ 中必有一个不被 p 整除,不妨设为 m_j,这时由引理 2.8.1 知,m_jg_j 和 g_j 的阶相等,都是 p^{r_j}. 考察集合

$$M=\{g_1,\cdots,g_{j-1},g_j'=m_ig_i+m_jg_j+m_tg_tz,g_{j+1},\cdots,g_k\}$$

重复上面的讨论可知,M 是 G 的生成元集,其元素个数为 k,仍是最小元素个数者. 另一方面,$p^sm_jg_j=l_jg_j\neq0$,因而 $p^s<p^{r_j}$,但 $p^sg_j'=0$,g_j' 的阶$\leqslant p^s$,这样按上面规定的次序,应有 $\{g_1,\cdots,g_k\}$ 大于 M,但这与我们对 $\{g_1,\cdots,g_k\}$ 的选择是矛盾的.

2)设 $\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_k=\mathbf{Z}h_1\oplus\cdots\oplus\mathbf{Z}h_s$. 对 g_i 的个数 k 作归纳法. 当 $k=1$ 时,由于 p-循环群不能再分解,故 $s=1$ 且 $Zg_1\cong Zh_1\cong G$.

设 $k>1$,且不妨设所有 g_i 中 g_k 的阶最大,记 g_k 的阶为 p^m,知所有 h_i 的阶中的最大数也是 p^m,否则用前面证明 p-循环群不可分解的方法可得出矛盾.

下面写出元素 g_k 用元素 h_i 表示的表达式:$g_k=l_1h_1+\cdots+l_sh_s$,不妨设 $h_j,h_{j+1},\cdots,h_s$ 是 h_i 中所有阶为 p^m 的元素,则它们在上式中的系数 $l_t,t=j,j+1,\cdots,s$,不能都被 p 整除,否则 g_k 的阶将小于 p^m. 不妨设 $(l_s,p)=1$,这时使用上面用过的方法,可以证明

$$G=\mathbf{Z}h_1\oplus\cdots\oplus\mathbf{Z}h_{s-1}\oplus\mathbf{Z}g_k.$$

另一方面,我们有

$$G=\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_{k-1}\oplus\mathbf{Z}g_k.$$

考察商群

$$G/\mathbf{Z}g_k\cong\mathbf{Z}g_1\oplus\cdots\oplus\mathbf{Z}g_{k-1}\cong\mathbf{Z}h_1\oplus\cdots\oplus\mathbf{Z}h_{s-1},$$

利用归纳法假设,便得 $k-1=s-1$,并且适当调整脚码后,有

$$\mathbf{Z}g_i\cong\mathbf{Z}h_i,i=1,2,\cdots,k-1.$$

另一方面,g_k 和 $h_s=h_k$ 同为阶为 p^m 的元素,当然也有 $\mathbf{Z}g_k\cong\mathbf{Z}h_k$,得证.

上述两个定理说明,任意给定的有限加群必是阶为素数幂的循环群的直和. 应该看一下问题的另一面,即存在性问题:是否存在有限加群,它是循环群的直和. 比如说,3

个 2 阶循环群和 7 个 5 阶循环群的直和？为了回答这个问题，我们引入

定义 2.6.3（外直积的定义）　设群 $G_i, i=1,\cdots,n$，令集合

$$G=G_1\times G_2\times\cdots\times G_n,$$

而规定集 G 中的一个二元运算如下：对 $g_i, h_i\in G_i, i=1,\cdots,n$，规定 $(g_1,\cdots,g_n)\cdot(h_1,\cdots,h_n)=(g_1h_1,\cdots,g_nh_n)$，这里 g_ih_i 是群 G_i 中的乘积. 直接验证 $(G,\cdot)$ 是一个群，称之为群 $G_1,\cdots,G_n$ 的（外）直积，记作

$$G=G_1\odot G_2\odot\cdots\odot G_n.$$

特别，当所有 G_i 是交换群时，G 也是交换群. 这时我们常把 G 写成 $G=G_1\oplus G_2\oplus\cdots\oplus G_n$，而称之为加群 G_i 的（外）直和.

这时 G 的运算用加法写成

$$(g_1,\cdots,g_n)+(h_1,\cdots,h_n)=(g_1+h_1,\cdots,g_n+h_n),$$

令

$$G'_i=\{(0,\cdots,0,g_i,0,\cdots,0)\mid g_i\in G_i\},$$

则 G_i 是 G 的子群，$G'_i\cong G_i$，且有 G 是其子群 $G'_i(i=1,\cdots,n)$ 的（内）直和. 在这个意义上内直和. 外直和是互通的，虽然内直和概念是属于结构理论的，而外直和是属于构造理论的.

上面的讨论肯定地回答了刚才所提出的关于有限加群的存在问题. 总结以上我们有下面这个漂亮的结果.

定理 2.6.4（有限交换群结构定理）　有限加群 G 可唯一地分解为素数幂循环群的直和，即设 $|G|=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t}$，$p_i$ 是不同素数，则

1) $G=G_{11}\oplus\cdots\oplus G_{1s_1}\oplus G_n\cdots\oplus G_{t1}\oplus\cdots\oplus G_{ts_t}$，其中 G_{ij} 是 $p_i^{m_{ij}}$ 阶循环群.

2) 自然数集 $(p_1^{m_{11}},\cdots,p_1^{m_{1s_1}},p_t^{m_{t1}},\cdots,p_t^{m_{ts_t}})$ 由群 G 唯一确定.

这是一个很值得欣赏的结构定理. 可以和算术基本定理相比. 那里表示任意整数的基本构件是“素数”，构造方法是“乘积”，而这里则是：表示任意有限加群的基本构件是“素数幂阶的循环群”，构造方法是“直和”. 在整数论中，自然数 n 的分解是

$$n=p_1^{m_1}p_2^{m_2}\cdots p_t^{m_t},$$

则在交换群论中，有限加群 G 的阶 $|G|=n$ 的分解是：

$$|G|=n=p_1^{m_{11}}\cdots p_1^{m_{1s_1}}p_t^{m_{t1}}\cdots p_t^{m_{ts_t}}.$$

问题 2.6

1. 设 H_1, H'_1, H_2 是 G 的子群. 如果 G 是 H_1 和 H_2 的内直积，也是 H'_1 和 H_2 的内直积. 求证：有群同构 $H_1\cong H'_1$. 试举反例说明，通常 $H_1\neq H'_1$.

2. 设群 G 是循环子群 $(a_1),\cdots,(a_n)$ 的内直积. 如果每个 a_i 的周期 m_i 都是正整数，

且 $m_1, m_2, \cdots, m_n$ 两两互素. 证明 G 是循环群.

3. 设 G 是群, $H_1, H_2, \cdots, H_n$ 是 G 的子群, 如果满足:

1) $G=H_1H_2\cdots H_n$;

2) $\forall\ h_i, h'_i \in H_i, i=1,2\cdots n$, 有 $(h_1,\cdots,h_n)(h'_1,\cdots,h'_n)=(h_1h'_1)\cdots(h_nh_n')$;

3) 如果 $g=g_1g_2\cdots g_n=g'_1g'_2\cdots g'_n$, 其中 $g_i, g_i' \in H_i, i=1,\cdots,n$ (此时称 g_i 是 g 在 H_i 中的分量)

那么称 G 是子群 $H_1, H_2, \cdots, H_n$ 的内直积. 求证: 如果 G 是子群 $H_1, H_2, \cdots, H_n$ 的内直积, 那么

(1) 对 $\forall\ h_i \in H_i$ 和 $h_j \in H_j$, 若 $i \neq j$, 则 $h_ih_j=h_jh_i$;

(2) H_i 是 G 的正规子群;

(3) 若 $i_1, i_2, \cdots, i_n$ 是 $1, \cdots, n$ 的一个排列, 则 G 也是 $H_{i_1}, \cdots, H_{i_n}$ 的内直积;

(4) 定义 $\varphi_i: G \to H_i \quad g \longmapsto h_i$

并称 φ_i 是 G 在 H_i 上的投影, 则投影 φ_i 是群的满同态, 且

$$\mathrm{Ke}\varphi_i = H_1\cdots H_{i-1}H_{i+1}\cdots H_n.$$

4. 设群 G 是子群 $H_1, H_2, \cdots, H_n$ 的内直积, 记

$$K=H_1 \odot H_2 \odot \cdots \odot H_n$$

是群 $H_1, H_2, \cdots, H_n$ 的外直积. 令 $\varphi: K \to G, g \longmapsto g_i$ (g_i 是 g 在 H_i 上的分量), 求证: φ 是群同构对应.

§2.7　有限群分类初步

代数学的基本问题之一就是决定某些公理定义的代数系统究竟有多少个互不同构的类型, 即所谓同构分类问题. 对于很多代数系统来说, 这个问题已经解决. 例如线性代数中的向量空间, 任意 n 维向量空间 $V_n(F)$ 都同构于 F^n. 这实际上就是域上有限向量性空间的同构分类定理. 它告诉我们, 从同构的意义上来说, 任意域上给定 n 维向量空间只有一个 F^n.

我们又有, 给定正整数 n, 任意两个 n 阶循环群彼此同构, 即从同构的意义上来说, n 阶循环群只有一个, 那就是 $\mathbf{Z}_n$. 这就是有限循环群的分类定理.

这样的例子还有许多, 基于同样的想法, Cayley 在给出了有限群的定义后, 于 1878 年明确地提出了对于一般的 n 阶有限群的同构分类问题. 与循环群的情形完全不同, 人们发现这个问题是非常复杂和困难的. 为了解决这个问题, 许多数学家经过艰苦的努力, 得到了若干个具有基本意义的有限群构造定理. 根据这些定理, 人们把解决有限群的同构分类问题归纳为以下两大步骤:

(1)分类所有的有限单群；

(2)找出"用单群来构造其他群"的方法.

这就是所谓的The Holder Program. 它为解决有限群的同构分类问题指明了方向并勾画了粗糙的轮廓. 因为，若群 G 有非平凡正规子群 N，则可构造一个比 G"小"的群 G/N. 而 N,G/N 的构造或多或少地能描述群 G 的构造. 虽然这种说法有些模糊，但至少它提示我们最强有力的数学技巧之一，数学归纳法可以使用. 我们经常对 N 和 G/N 使用归纳假设以得到许多有用的结果.

在某种意义上，有限单群是构造有限群的"基元素"，为了使用这"基元素"来证明有限群的一般定理，我们需要了解关于有限单群的详尽信息. 值得庆幸的是，分类所有的有限单群的工作，通过数百位数学家数十年的努力，已于 1980 年宣告完成. 目前该项工作正在简化、整理. 这一工作被认为是 20 世纪数学界获得的最伟大的成就之一. 对于 The Holder Program 的第二部分，进展缓慢，仍有大量艰难工作要做. 为了介绍 Jordan-Holder 定理，先介绍一些概念及预备知识.

定义 2.7.1　称群 G 的子群列 $1=G_0\leqslant G_1\leqslant G_2\leqslant\cdots\leqslant G_r=G$ 为 G 的合成群列. 对 $\forall\, i$，每个商群 G_{i+1}/G_i 为单群. 称上面的合成群列的长度为 r. 合成群列中的商群称为这一群列的合成因子.

更一般地，一个群称为群 G 的合成因子，若它同构于 G 的某一合成列中的一个合成因子.

例如，考虑群 S_5，A_5 是 S_5 的唯一的非平凡正规子群. 由于 $S_5/A_5\cong\mathbf{Z}_2$，也是单群，故 $1\lhd A_5\lhd S_5$ 为 S_5 的一个合成群列.

定义 2.7.2　称 N 为群 G 的极大正规子群，若 $N\lhd G$，且 G 没有真包含 N 的正规子群.

任意非平凡有限群均有极大正规子群. 由对应定理易见，N 是 G 的极大正规子群当且仅当 G/N 是单群. 正规的极大子群必然是极大正规子群(且指数为素数)，但极大正规子群不一定是极大子群，因为它可能真含于一个非正规真子群中.

例如，群 $1\times\mathbf{Z}_2$ 是 $A_5\times\mathbf{Z}_2$ 的极大正规子群，但不是极大子群. 一个群是否一定有合成群列呢？我们有下面的

定理 2.7.1　有限群有合成群列.

证明　设 G 是有限群，对 $|G|$ 作归纳法. 若 G 是单群，则 $1\lhd G$ 是 G 的合成群列；否则 G 有极大正规子群 G'，由假设，G' 有合成群列

$$1=G_0\leqslant G_1\leqslant G_2\leqslant\cdots\leqslant G_r=G$$

由于 G/G' 是单群，故

$$1=G_0\leqslant G_1\leqslant\cdots\leqslant G'\leqslant\cdots\leqslant G_r=G$$

是 G 的合成群列.

无限群不一定有合成群列. 例如, 令 G 是无限循环群, 因为 G 的每个非平凡子群均为无限循环群, 因而均同构于 G. 由于 G 非单群, 故 G 没有子群是单群. 由于 G 的合成群列的最后一个非平凡项必为 G 的单子群, 因而不能构造出 G 的合成群列.

引理 2.7.2　设 $N \lhd G$, 若 G 有合成群列, 则 N 有合成群列.

证明　设 $1=G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_r=G$ 是 G 的合成群列. 令 $N_i=N \cap G_i$, 对任意 i, 这样得到 N 的一个子群列 $1=N_0 \leqslant N_1 \leqslant \cdots \leqslant N_r=N$, 固定某一 i, 易见 $N_i \lhd N_{i+1}$, 由 $N \cap G_i=(N \cap G_{i+1}) \cap G_i$ 及第一同构定理得

$$N_{i+1}/N_i=(N \cap G_{i+1})/(N \cap G_i) \cong (N \cap G_{i+1})G_i/G_i.$$

设 $\varphi: G_{i+1} \to G_{i+1}/G_i$ 为自然同态, 则

$$(N \cap G_{i+1})G_i/G_i=\varphi(N \cap G_{i+1}) \lhd \varphi(G_{i+1})=G_{i+1}/G_i$$

因而 N_{i+1}/N_i 同构于单群 G_{i+1}/G_i 的一个正规子群, 因此 $N_{i+1}=N_i$ 或 $N_{i+1}/N_i \cong G_{i+1}/G_i$ 为单群, 所以去掉子群列 $1=N_0 \leqslant N_1 \leqslant \cdots \leqslant N_r=N$ 中的重复项后, 就得到 N 的一个合成群列.

设 $1=G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_r=G$ 是合成群列, $1=H_0 \leqslant H_1 \leqslant H_2 \leqslant \cdots \leqslant H_r=G$ 也是长度为 r 的另一合成群列, 称这两个群列是等价的:

若存在 $\pi \in S_r$, 使对每个 i, $G_i/G_{i-1} \cong H_{\pi(i)}/H_{\pi(i)-1}$.

例如, $G=\langle x \rangle \cong \mathbf{Z}_6$, $G_1=\langle x^2 \rangle$, $H_1=\langle x^3 \rangle$, 考虑合成群列 $1 \lhd G_1 \lhd G$ 和 $1 \lhd H_1 \lhd G$, 由于 $G/G_1 \cong H_1/1 \cong \mathbf{Z}_2$, $G_1/1 \cong G/H_1 \cong \mathbf{Z}_3$ (取 $\pi=(12) \in S_2$), 故它们等价.

在等价的意义下, 一个群仅有唯一的合成群列. 因此, 有合成群列的群其合成因子构成的集合是唯一确定的, 对这些合成因子的了解直接影响对这个群的结构的了解. 由于合成因子均是单群, 所以在研究任意有限群时, 首先应对有限单群有一非常好的理解.

Jordan-Holder 定理　若群 G 有合成群列, 则 G 的任意两个合成群列有相同的长度, 且它们等价.

证明　设 $1=G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_r=G$; $1=H_s \leqslant \cdots \leqslant G_1 \leqslant G_0=G$ 是 G 的两个合成群列. 对 r 作归纳法. 若 $r=1$, 则 G 是单群.

显然, $1 \lhd G$ 是 G 的唯一的合成群列.

设 $r>1$, 且对任意合成群列长度小于 r 的群来说, 结论成立. 若 $G_1=H_1$, 则 G_1 有两个长度分别为 $r-1$ 和 $s-1$ 的合成群列. 由归纳假设得 $r=s$, 且 G_1 的两个合成群列等价, 从而 G 的这两个合成群列等价.

下设 $G_1 \neq H_1$, 由于 $G_1 \lhd G$, $H_1 \lhd G$, 则 $G_1H_1 \lhd G$, 但 G/G_1 是单群, 故不能有 $G_1 < H_1$, 从而 $H_1 < G_1H_1$, 由 G/H_1 的单性得 $G_1H_1=G$. 令 $K=G_1 \cap H_1 \lhd G$, 由第一同构定理

可知 $G/G_1 \cong H_1/K, G/H_1 \cong G_1/K$(特别地,$G_1/K, H_1/K$ 为单群). 由引理 2.7.2 可知 K 有合成群列. 不妨设 $1=K_t \leqslant \cdots \leqslant K_1 \leqslant K_0 = K$ 为 K 的一个合成群列.

现在得到 G_1 的两个合成群列

$$1=G_0 \leqslant G_1 \leqslant G_2 \leqslant \cdots \leqslant G_r \text{ 和 } 1=K_t \leqslant \cdots \leqslant K_1 \leqslant K \leqslant G_1$$

它们的长度分别为 $r-1$ 和 $t+1$,由归纳假设得 $t=r-2$,且这两个合成群列等价. 同理可得 H_1 有两个合成群列

$$1=H_s \leqslant \cdots \leqslant H_2 \leqslant H_1 \text{ 和 } 1=K_{r-2} \leqslant \cdots \leqslant K_1 \leqslant K \leqslant H_1$$

长度分别为 $s-1$ 和 $r-1$,由归纳假设可得 $r=s$,且这两个合成群列等价.

结合上面得到的同构可知,合成群列

$1=K_{r-2} \leqslant \cdots \leqslant K \leqslant G_1 \leqslant G_0 = G$ 和 $1=K_{r-2} \leqslant \cdots \leqslant K \leqslant H_1 \leqslant H_0 = G$ 等价,所以群 G 原来的两个合成群列等价.

合成群列仅仅是在群论研究中起着很重要作用的一类子群列,下面我们介绍更一般的一些子群列.

定义 2.7.3　群 G 的一个子群列 $1=G_r \leqslant \cdots \leqslant G_1 \leqslant G_0 = G$ 称为次正规群列,对$\forall i$ 有 $G_{i+1} \lhd G_i$.

定义 2.7.4　一个次正规群列称为正规群列,若对每个 i 有 $G_i \lhd G$.

合成群列是次正规群列的一个特例,但反之不然,因为次正规群列可能有平凡的商群因子,或者有非平凡商群因子,但不是单群.

定义 2.7.5　两个长度相同的次正规群列称为等价的,若它们满足合成群列等价定义中所给出的条件.

定义 2.7.6　一个给定的次正规群列经过插入子群所得到的新的次正规群列称为原来次正规群列的加细.

若所插入的项中至少有一个在原来的群列中没有出现,称为真加细. 因而合成群列是没有重复项的且没有真加细的次正规群列.

定义 2.7.7　群 G 的正规群列称为主群列,若该正规群列中没有重复项,且任意两项之间不能再插入其他的正规子群(注意:合成群列是没有真加细的次正规群列,主群列是没有真加细的正规群列).

定义 2.7.8　群 G 的主群列中相邻两群作成的商群称为 G 的主因子. 一个群称为群 G 的主因子,若它同构于群 G 的某一主群列中的一个主因子.

对主群列也有类似的 Jordan-Holder 定理,即一个群的任意两个主群列都有相同的长度,且等价. 其证明类似于合成群列情形的证明.

这两个结果是算子群的 Jordan-Holder 定理的特殊情形.

定义 2.7.9　称 N 为群 G 的极小正规子群,若 $1 \neq N \lhd G$,且 N 不真包含 G 的非平

凡正规子群.

任意非平凡有限群有极小正规子群;单群的唯一极小正规子群是它自身.

定理 2.7.3 有限群有主群列.

证明 设 G 是有限群,对 $|G|$ 作归纳法,若 G 为单群,则 $1\lhd G$ 是 G 的主群列,否则,G 有非平凡极小正规子群 N. 由归纳假设,G/N 有主群列,由对应定理可知这一主群列有形式:

$$1=G_r/N\lhd \cdots\lhd G_1/N\lhd G_0/N=G/N$$

其中对 $\forall\ i, G_i\lhd G$,且在 G_i 与 G_{i-1} 之间没有 G 的非平凡正规子群. 由于 N 是 G 的极小正规子群,故 $1\lhd N=G_r\lhd \cdots\lhd G_1\lhd G_0=G$ 是 G 的主群列.

由定义知,有限群的合成因子均是单群. 在本节的最后,我们来决定有限群的主因子. 首先有下面的引理

引理 2.7.4 G 有主群列,则 G 的每个主因子是 G 的某商群的极小正规子群.

证明 若 $1=G_r\lhd \cdots\lhd G_1\lhd G_0=G$ 是 G 的一个主群列,由对应定理可知每个 C_i/G_{i+1} 是 G/G_{i+i} 的极小正规子群.

定理 2.7.5 有限群的极小正规子群是同构单群的直积.

证明 设 G 是有限群,N 为 G 的极小正规子群. 设 N_1 是 N 的极大正规子群,故 N/N_1 是单群. 设 $N_1, N_2, \cdots, N_r$ 是 N_1 在 G 中的所有共轭子群,由于 $N\lhd G$,故每个 N_i 为 N 的极大正规子群. 若 $x\in G, N_i=xN_1x^{-1}$,则 N/N_1 到 N/N_i 的映射 $\varphi: gN_1\longmapsto xgx^{-1}N$ 是同构映射,说明所有 N/N_i 是互相同构的. 由于 $N_1\cdots N_r$ 是 N_1 在 G 中所有的共轭子群,故对 $g\in G$,g 保持集合 $\{N_1,\cdots,N_r\}$ 不动,因而

$$g(N_1\cap \cdots\cap N_r)g^{-1}=Gn_1g^{-1}\cap\cdots\cap gN_rg^{-1}=N_1\cap \cdots\cap N_r$$

故 $N_1\cap \cdots\cap N_r\lhd G$,但 $N_1\cap \cdots\cap N_r\leqslant N$,由 N 的极小性得 $N_1\cap \cdots\cap N_r=1$.

对每个 $1\leqslant i\leqslant r$,群 $N/(N_1\cap \cdots\cap N_r)$ 是同构于 N/N_1 的某些群的直积. 从而令 $i=r$,即得结论成立.

对 i 作归纳法,当 $i=1$ 时,显然成立;设 $i>1$,且对 $i-1$ 结论成立,若 $N_1\cap \cdots\cap N_{i-1}\leqslant N_i$,则 $N_1\cap \cdots\cap N_i=N_1\cap \cdots\cap N_{i-1}$,结论显然成立.

因此我们假设 $N_1\cap \cdots\cap N_{i-1}\not\subset N_i$,此时

$$N_i<(N_1\cap \cdots\cap N_{i-1})N_i\lhd N.$$

又由于 N_i 是 N 的极大正规子群,必有

$$(N_1\cap \cdots\cap N_{i-1})N_i=N$$

则

$$N/(N_1\cap\cdots\cap N_i)=(N_1\cap\cdots\cap N_{i-1})/(N_1\cap\cdots\cap N_i)\times N_i/(N_1\cap\cdots\cap N_i)$$

但由第一同构定理有

$$(N_1\cap \cdots\cap N_{i-1})/(N_1\cap \cdots\cap N_{i-1})\cap N_i$$

$\cdot \cong (N_1 \cap \cdots \cap N_{i-1})N_i/N_i = N/N_i \cong N/N_1$.

类似地有

$N_i/(N_1 \cap \cdots \cap N_{i-1}) \cap N_i$

$\cong (N_1 \cap \cdots \cap N_{i-1})N_i/(N_1 \cap \cdots \cap N_{i-1}) = N/(N_1 \cap \cdots \cap N_{i-1})$.

由归纳假设即得结论成立.

推论 2.7.6　有限群的主因子是同构单群的直积.

问题 2.7

1. 证明：交换群 G 有合成群列当且仅当 G 是有限群.
2. 对于 $n>2$，决定 S_5 的所有合成群列和主群列.
3. 证明：有合成群列的群一定有主群列.
4. $H \lhd$ 有限群 G，证明 G 有一个合成群列，它的其中一项是 H.
5. 证明：若下列条件之一成立，则群 G 不是单群：

(1) $|G| = p^a(p+1)$，其中 $a>1$；

(2) $|G| = p^a(p+3)$，其中当 $p=2$ 时，$a>3$；当 $p>3$ 时，$a \geqslant 1$；

(3) $|G| = p^a(p^2-1)$，其中 $a>1$，p 为奇素数.

6. 若 $|G| \in \{30, 56, 105, 132\}$，则 G 不是单群.
7. 设 G 为有限群，$H \leqslant G$，$P \in \mathrm{Sylow}_p(H)$，证明：若 $N_G(P) \leqslant H$，则 $P \in \mathrm{Sylow}_p(G)$.
8. 证明：p^2 阶群是交换群，其中 p 为素数.
9. 设 P 为有限 p 群，N 为 P 的交换正规子群中的极大者，证明：$N = C_P(N)$.

§2.8　可解群

上节我们引进了群的各种子群列的概念. 本节将利用子群列来研究群. 特别地，利用子群列来定义一类重要的群——可解群. Galois 引进群的概念，研究 5 次及 5 次以上方程的根式解问题，他证明了 $n(n \geqslant 5)$ 次方程有根式解当且仅当这个方程的 Galois 群是可解群，因而可解群是令人感兴趣的一类群. 本节将考察这类群及其相关群类.

定义 2.8.1　设 G 是群，令 $G^{(0)} = G$，对 $k \in \mathbf{N}$，定义 $G^{(k)}$ 为 $G^{(k-1)}$ 的导群，所得到的群列称为 G 的导群列.

对$\forall$ k，$G^{(k+1)}$ 为 $G^{(k)}$ 的特征子群；导群列是 G 的一个正规群列，而且导群列中任意相邻两群的商群都是交换群.

定义 2.8.2　称一个群为可解群，若它的导群列终止于 1(可解群的定义是 Galois

于 1830 年在研究多项式的根式解过程中提出的，事实上，这就是“可解”这一术语的来源).

由于一个群为交换群当且仅当其导群为 1. 易见，交换群为可解群. 但是并不是所有群都可解. 例如，A_5 不是可解群. 由于单群几乎没有正规子群，而可解群有许多正规子群，故可解群可认为是与单群相反的一个概念. 如果这一思想正确的话，那么就应该有很少的群既是单群又是可解群，而事实正是如此.

定理 2.8.1　可解单群为素数阶循环群.

证明　设 G 为可解单群，由于 G 是可解群，故 $G'\neq G$；又因为 G 是单群，故 $G'=1$，从而 G 为交换群. 但由于交换单群的每个非单位元必是生成元，故 G 必为素数阶循环群.

下面给出可解群的一些性质.

定理 2.8.2　设 G 是群，则下列条件等价：

(1)G 是可解群；

(2)G 有一个正规群列，其相邻两群构成的商群为交换群；

(3)G 有一个次正规群列，其相邻两群构成的商群为交换群.

证明　(1)⇒(2)⇒(3)显然，故只需证(3)⇒(1).

设 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_r=1$ 是 G 的次正规群列，且任意相邻两群构成的商群为交换群，因为 $G_r=1$. 要证明 G 可解，只需证对$\forall\ i, G^{(i)}\leqslant G$ 成立即可.

对 i 作归纳法. 由于 G/G_i 交换，则 $G^{(1)}\leqslant G_1$. 设 $i>1$，由归纳假设得 $G^{(i-1)}\leqslant G_{i-1}$，则 $G^{(i)}=(G^{(i-1)})'\leqslant(G_{i-1})'$，由于 G_{i-1}/G_i 交换，则$(G_{i-1})'\leqslant G_i$，故 $G^{(i)}\leqslant C_i$.

下面我们来考察一下与可解群相关的一些群的可解性.

定理 2.8.3　设 G 是群，则：

(1)若 G 可解，$H\leqslant G$，则 H 可解；

(2)若 G 可解，$N\lhd G$，则 G/N 可解；

(3)若 $N\lhd G$，且 $N, G/N$ 可解，则 G 可解；

(4)若 G, H 可解，则 $G\times H$ 可解.

证明　(1)由于对$\forall\ k$，有 $H^{(k)}\leqslant G^{(k)}$，故(1)成立；

(2)存在正规群列

$$G=C_0\geqslant G_1\geqslant\cdots\geqslant G_r=1,$$

使得对每个 i，G/G_{i+1}为交换群，考虑群列

$$G/N=G_0N/N\geqslant G_1N/N\geqslant\cdots\geqslant G_rN/N=1,$$

固定某个 i，由于 $G_i\lhd G, N\lhd G$，故 $C_iN\lhd G$，因而 $G_iN/N\lhd G/N$，由于 $G_iN=G_i(G_{i+1}N)$，由第一和第二同构定理可得

$$(G_iN/N)/(C_{i+l}N/N)\cong G_iN/G_{i+1}N\cong G_i/(G_i\cap G_{i+1}N)$$

又由第二同构定理知，$G_i/(G_i\cap G_{i+1}N)$同构于交换群 G_i/G_{i+1} 的一个商群，因此是交换群. 这样我们构造出 G/N 的一个正规群列，其任意两群构成的商群均为交换群，由定理 2.8.2 知 G/N 可解；

(3)存在次正规群列

$$N=N_0\geqslant N_1\geqslant \cdots\geqslant N_r=1$$

和

$$G/N=G_0N/N\geqslant G_1N/N\geqslant \cdots\geqslant G_sN/N=1,$$

对$\forall\ i$，N_i/N_{i+1}交换，且$(G_i/N)/(G_{i+1}/N)\cong G_i/G_{i+l}$也交换.

易见

$$G=C_0\geqslant G_l\geqslant \cdots\geqslant C_s=N=N_0\geqslant N_1\geqslant \cdots\geqslant N_r=1$$

是 G 的次正规群列，且任意两群构成的商群均为交换群，则 G 为可解群；

(4)此时 $1\times H\cong H$ 是 $G\times H$ 的可解正规子群，$G\times H/1\times H\cong G$ 也可解. 由(3)可知 $G\times H$ 可解.

由定理易知，对称群 S_2,S_3,S_4 均为可解群，而 S_5 不是可解群.

定理 2.8.4　有合成群列的群是可解群⇔它的所有合成因子为素数阶.

证明　设 G 是有合成群列的群，若 G 的所有合成因子均为素数阶群，则这个合成群列为 G 的一个次正规群列，其任意两群构成的商群均为交换群，由定理 2.8.2 知 G 可解；反之，设 G 是可解群，H/K 为 G 的合成因子，其中 $K\lhd H\leqslant G$，由定理 2.8.3 的(1)，(2)可知 H/K 可解. 从而 H/K 是可解单群，由定理 2.8.1 知，H/K 为素数阶.

易见，存在既非单又不可解的群，如 S_5，也存在非交换的可解群，如 S_3(其合成群列为 $S_3>A_3>1$). 没有合成群列的群有可能是可解群，例如，无限交换群是可解群，但它没有合成群列.

定理 2.8.5　有限 p 群是可解群.

证明　由于有限 p 群的合成因子为单群且为 p 群，故为素数阶群，由定理 2.8.4 得结论成立.

由定理 2.8.4 可知，可解群的所有合成因子为素数阶，那么如果有主群列的群是可解群的话，它的每个主因子又怎样呢？

定义 2.8.3　设 p 是素数，Z_p 是 p 阶循环群，n 是正整数，则 n 个循环群 Z_p 的直积 $Z_p\times Z_p\times \cdots\times Z_p$ 称为 p^n 阶初等交换 p 群.

容易验证，有限交换群 G 是初等交换 p 群的充要条件是 $\exp(G)=p$.

定理 2.8.6　有主群列的群是可解群⇔它的每个主因子为初等交换 p 群.

证明　设群 G 有主群列，若 G 的所有主因子为初等交换 p 群，则可加细群 G 的主

群列，得到群 G 的一个合成群列，它的合成因子均为素数阶，由定理 2.8.4 可知，G 是可解群.

反之，若 G 可解，设 H/K 为 G 的一个主因子，其中 $K\lhd H\lhd G$. 又由定理 2.8.3 可知，H/K 为可解群，而由定理 2.8.4 可得，H/K 的每个合成因子为素数阶，因而 H/K 有限. 由推论 2.7.6 知，H/K 为同构于某一单群 S 的若干个群的直积. 由于 H/K 的每个合成因子必同构于 S，且这些因子为素数阶，故 H/K 是初等交换 p 群.

定理 2.8.7　有合成群列的群是可解群当且仅当它有一正规群列其相邻两群构成的商群为 p 群.

证明　设群 G 有合成群列，假设 G 有一正规群列，其相邻两群构成的商群为 p 群，加细这一正规群列得到群 G 的主群列. 易见群 G 的每个主因子是 p 群的一个截断（群 G 的任意子群的商群称为 G 的一个截断），从而 G 的每个主因子为 p 群，由推论 2.7.6 知，每个主因子是同构单群的直积，从而每个主因子必是初等交换 p 群，则 G 可解. 另一方面，由定理 2.8.6 直接可得.

定义 2.8.4　主因子为素数阶循环群的有限群称为超可解群.

因为有限超可解群为可解群且有限 p 群为超可解群. 但是并非所有的有限可解群均为超可解群.

例如，S_4 有主群列 $S_4>A_4>K>1$，其中 K 为 Klein 四元群，且 $S_4/A_4\cong Z_2$，$A_4/K\cong Z_3$，$K\cong Z_2\times Z_3$，由定理 2.8.6 知 S_4 是可解群，但不是超可解群.

可解群有许多对任意有限群成立的性质，下面由 Phillip Hall 给出的定理是 Sylow 定理在有限可解群中的一个推广. 为了证明这个定理，我们先介绍一些概念，并不加证明地给出有限群中的一个基本定理.

定义 2.8.5　群 G 的正规子群 N 在 G 中的补子群是指群 G 的子群 H，满足 $G=NH$，且 $N\cap H=1$.

定义 2.8.6　有限群 G 的子群 H 称为 Hall 子群，若 $|H|$ 与 $[G:H]$ 互素.

Schur-Zassenhaus 定理　有限群的任意正规 Hall 子群均有补子群.

定理 2.8.8　设 G 是有限可解群，其阶为 mn，其中 $(m,n)=1$，则：

(1) G 有 m 阶子群；

(2) G 的任意两个 m 阶子群均共轭；

(3) 群 G 的阶整除 m 的子群包含在 G 的某一个 m 阶子群中.

证明　设 G 满足题设，对 $|G|$ 作归纳法，假设结论对阶小于 $|G|$ 的所有群均成立. 设 N 为 G 的极小正规子群，则 N 为 G 的主因子，故由定理 2.8.6 知，N 为初等交换 p 群，p 为素数. 由于 $(m,n)=1$，且 $p|mn$，故 p 只能整除 m,n 中的一个. 若 $p\mid m$，则 $|G/N|=(m/|N|)n$ 是互素的两个整数的乘积. 由归纳假设，G/N 有 m 阶子群，由对应定理可

知，G 有 m 阶子群. 若 $p \mid n$，同理可得 G/N 有 m 阶子群 H/N. 这时 $|H|=m|N|$ 是互素的两个整数的乘积. 若 $H<G$，由归纳假设，H 有 m 阶子群，从而 G 也有 m 阶子群. 若 $H=G$，由于 N 是 G 的正规子群，且 $|H|=n$ 和 $[G:N]=m$ 互素，由 Schur-Zassenhaus 定理可知结论成立.

这个定理对任意有限群不一定成立，例如，A_5 就没有 20 阶子群.

下面我们不加证明地给出有限群为可解群的一些著名定理.

Burnside 定理　设 p,q 是素数，a,b 为非负整数，则 p^aq^b 阶群可解.

Burnside 定理是一个非常典型的结果，它告诉我们阶有 3 个因子的有限群不一定可解，且 A_5 就是一个反例.

Feit-Thompson 定理　奇阶群是可解群.

这个定理也称为“奇阶定理”，首先是由 Burnside 在 1911 年提出的猜想，作为推论，易见奇阶单群只能是素数阶循环群.

定理 2.8.9　设 G 是有限群，若 G 有 m 阶子群，且 $|H|=mn$，其中 $(m,n)=1$，则 G 是可解群.

定理 2.8.10　有限群 G 不可解 $\Leftrightarrow$ 存在 G 的阶互素的非单位元 x,y,z 使得 $xy=z$.

例如，在 A_5 中取 $x=(1\ 2\ 3\ 4\ 5)$，$y=(1\ 2)(3\ 4)$，$z=(2\ 4\ 5)$，其中 $|x|=5$，$|y|=2$，$|z|=3$，则 A_5 满足定理 2.8.10 的条件，从而知 A_5 不可解.

Thompson 小传

汤普森(J. G. Thompson)，美国数学家，1932 年 10 月 13 日生于堪萨斯州的渥太华. 1951 年作为神学专业学生进入耶鲁大学，但二年级时转为数学专业. 1955 年到芝加哥大学攻读博士，四年后获博士学位. 在哈佛大学任教了一年之后，1962 年回到芝加哥大学任教授. 1968 年到英国剑桥大学. 1993 年起任佛罗里达大学教授. 1971 年被选为美国全国科学院院士. 1979 年被选为英国皇家学会会员.

1959 年，Thompson 在他的博士论文中证明了一个有 50 年历史的有关有限群的自同构的弗罗贝尼乌斯猜想，并用该论文中的方法在 1963 年与费特(W. Feit)合作证明了有限群的伯恩塞德猜想：有限非 Abel 单群必为偶数阶的，或等价地说，每一个奇数阶群都是可解群. 发表这一成果的论文长达 225 页，占了《太平洋数学杂志》整整一期. 这一结果标志着有限单群分类的重大突破. 他所获得的结果以及证明中所用到的新方法在 20 世纪 60 年代和 70 年代被许多数学家应用和推广，最终导致了 80 年代有限单群分类问题的彻底解决.

20 世纪 70 年代后期，Thompson 还在编码理论、有限射影平面理论以及模函数论中有过重要的贡献. 他最近有关伽罗瓦群的工作被认为是域论中最重要的工作之一. 他

曾荣获美国数学会科尔代数奖(1966)、菲尔兹奖(1970)、沃尔夫奖(1992)、法国科学院授予的庞加莱金质奖章(1992)以及美国国家科学奖(2000).

问题 2.10

1. 设 $G=N\times H, N\leqslant K\leqslant G$, 求证: $K=N\times(H\cap K)$.
2. 设 $G=H\times N$, 求证: A 的正规子群也是 G 的正规子群.
3. 证明: 有限群有一个极大可解正规子群.
4. 证明: $\mathrm{Aut}(\mathbf{Z}_8)\cong Z_2\times Z_2$.
5. 证明: 如果 P 是非循环有限 p 群, 则有 $N\lhd P$, 使得 $P/N\cong Z_p\times Z_p$.
6. 证明: 有限群 G 是超可解群 $\Leftrightarrow$ 它有一个正规列, 每个商因子为循环群.
7. 设 G 是满足极大条件的群, 当 G 的自同构群 $\mathrm{Aut}(G)$ 是超可解群时, 证明 G 是超可解的.

§2.9　幂零群与超可解群

本节介绍群论中的另一个重要群类, 它介于交换群与可解群之间.

定义 2.9.1　群 G 的一个正规群列 $G=G_0\geqslant G_1\geqslant\cdots\geqslant C_r=1$ 称为 G 的中心群列, 若对每个 i, G_i/G_{i+1} 包含在 G/G_{i+1} 的中心里.

定义 2.9.2　若群 G 有一个中心群列, 称 G 为幂零群.

交换群 G 有中心群列 $G>1$, 从而交换群是幂零群.

定义 2.9.3　群 G 有一个有限的正规群列 $G=G_0\geqslant G_1\geqslant\cdots\geqslant C_r=1$, 其中每个商群 G_i/G_{i+1} 都是循环群, 则称 G 为超可解群.

定理 2.9.1　幂零群是可解群.

证明　设 G 是幂零群, 则 G 有中心群列, 从而 G 有商因子为交换群的正规群列, 易知 G 是可解群, 存在可解但非幂零的群. 例如, S_3 没有中心群列. 否则, 这样的群列中的倒数第二项必为 $Z(S_3)$ 的非平凡子群, 显然这不可能. 故 S_3 不是幂零群.

定理 2.9.2　有限幂零群是超可解群.

证明　设 G 为有限幂零群, $G=G_0\geqslant G_1\geqslant\cdots\geqslant C_r=1$ 是 G 的一个中心群列. 若把这个中心群列加细为主群列, 则它仍为 G 的一个中心群列. 由于包含于群 G 的中心里的子群必为 G 的正规子群, 故 G 的主群列就是它的合成群列, 因而列中每个商群为素数阶循环群, 从而 G 为超可解群.

定理 2.9.3　超可解群的子群和商群是超可解的.

证明　设 G 是超可解群, 而且 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_r=1$ 是正规群列, 其中每个 $G_i/$

G_{i+1}都是循环群，那么对于商群 $G/K=T$，G_i 的同态像 H_i 组成正规群列

$$T=H_0\geqslant H_1\geqslant\cdots\geqslant H_r=1,$$

这里在把重复的群删去后，对于相邻的项 H_i 和 H_{i+1} 就一定有循环的商群 H_i/H_{i+1}，因为循环群的同态像是循环群或单位元群. 对于子群 N，取 $N=N_0\geqslant N_1\geqslant\cdots\geqslant N_r=1$，这里 $N_i=N\cap G_i$. 对于 $\forall\ i$，$N\cap G_i$ 在 H 内是正规的，而且，

$$N_i/N_{i+1}=N\cap G_i/N\cap G_{i+1}\cong G_{i+1}\cup(N\cap G_i)/G_{i+1}.$$

但是右端是 G_i/G_{i+1} 的子群，因而是循环群或单位元群，因此 N_i/N_{i+1} 是循环群或单位元群，所以 N 是超可解群.

推论 2.9.4　超可解群满足极大条件.

超可解群是有限生成的，因而根据以上定理，它的子群也是有限生成的，所以极大条件满足.

定理 2.9.5　超可解群 G 具有正规群列 $G=H_0\geqslant H_1\geqslant\cdots\geqslant H_k=1$. 其中每个商群 H_i/H_{i+1} 是无限循环群或是素数阶循环群.

证明　设 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_r=1$ 是正规群列，其中 G_{i-1}/G_i 是循环群，如果 G_{i-1}/G_i 是有有限的阶 $p_1p_2\cdots p_s$，其中 $p_1,p_2\cdots p_s$ 是素数(不必须是不同的)，则 G_{i-1}/G_i 具有阶为 $p_1,p_1p_2,\cdots,p_1\cdots p_{s-1}$ 的唯一循环子群，而且这些都是特征子群，因此在 G_{i-1} 和 G_i 之间的 $s-1$ 个对应的子群在 G 内是正规的，而且相邻的群的商群是素数阶循环群. 用这个方法加细每个有限阶的商群 G_{i-1}/G_i，就得出定理中的正规群列，其中每个商群是无限循环群或素数阶循环群.

这个定理还可以进一步加强而按素数的大小来重新排列素数阶商群.

定理 2.9.6　超可解群的导出群是幂零的.

证明　设 $G=G_0\geqslant G_1\geqslant\cdots\geqslant G_r=1$ 是 G 的正规群列，其中 G_{i-1}/G_i 是循环群，记 $H_i=G'\cap G_i$，那么 $G'=H_0\geqslant H_1\geqslant\cdots\geqslant H_r=1$ 是正规序列，而且这序列中不同的项 k_i 组成群列 $G'=K_0\geqslant K_1\geqslant\cdots\geqslant K_s=1$，其中 K_{i-1}/K_i 是循环群. 我们来断定这些 K 组成 G' 的中心群列.

每个 K_i 是 G 中一些正规子群的交，因此在 G 内是正规的，这时 G/K_i 内 K_{i-l}/K_i 是循环的正规子群，用 G/K_i 的元素作变形导出循环群 K_{i-1}/K_i 的自同构. 然而循环群的自同构组成 Abel 群，所以 G/K_i 的两个元素导出 K_{i-1}/K_i 的可交换的自同构. 于是任何两个元素的换位子 $x^{-1}y^{-1}xy$ 导出 K_{i-1}/K_i 的恒等自同构. 这说明 K_{i-1}/K_i 属于 G'/K_i 的中心，因而这些 K 组成 G' 的中心群列，所以 G' 是幂零的.

定理 2.9.7　有限 p 群是幂零群.

证明　设 P 为有限 p 群，对 $|P|$ 作归纳法. 若 $|P|=p$，则 P 为交换群，从而幂零；若 $|P|>p$，令 $Z=Z(P)$，则 $Z\neq 1$. 由归纳假设知，P/Z 有中心群列

$$P/Z=P_0/Z\geqslant P_1/Z\geqslant\cdots\geqslant P_r/Z=1,$$

易见群列 $P=P_0\geqslant P_1\geqslant\cdots\geqslant P_r=Z\geqslant 1$ 是 P 的中心群列.

定理 2.9.8 设 G 是有限群,则下列陈述等价:

(1)G 是幂零群;

(2)对 G 的任意子群 H,有 $N_G(H)>H$;

(3)G 的每个 Sylow 子群在 G 中正规;

(4)G 是其Sylow 子群的直积;

(5)G 的每个极大子群在 G 正规.

证明 首先我们证明,(3),(4),(5)等价.

假设(3)成立.设 $p_1,\cdots,p_n$ 是 $|G|$ 的不同的素因子,对每个 $1\leqslant i\leqslant n$,设 p_i 只为 G 的 Sylowp_i-子群,由假设知 $p_i\leqslant G$.由 Lagrange 定理,对$\forall\ i,P_1P_2\cdots P_i$ 是阶为 $|P_1||P_2|\cdots|P_i|$ 的正规子群,这说明 $G=P_1P_2\cdots P_n$.

同理可证,对$\forall\ i,|P_1\cdots P_{i-1}P_{i+1}\cdots P_n|=|P_1|\cdots|P_{i-1}||P_{i+1}|\cdots|P_n|$,因而 $P_i\cap(P_1\cdots P_{i-1}P_{i+1}\cdots P_n)=1$,所以 G 为所有 P_i 的直积.(5)得证.

设(4)成立,M 为 G 的极大子群,$P_1,P_2,\cdots,P_n$ 为 G 的 Sylow 子群,M 是诸 $M\cap P_i$ 的直积.由于 M 是 G 的极大子群,只存在一个 j,使得 $M\cap P_j$ 是 P_j 的极大子群,而对其他 $i\neq j$,有 $M\cap P_i=P_i$,则 $M\cap P_j\leqslant P_j$,从而 $M\leqslant G$.

若(5)成立,设 G 为的非正规的Sylow 子群,则有 $P\leqslant N_G(P)<G$,从而存在 G 的极大子群 M,使得 $P\leqslant N_G(P)\leqslant M$.由于 P 为 M 的 Sylow 子群,且由假设知 $M\leqslant G$,根据 Frattini 论断可得 $G=N_G(P)M=M$,矛盾,从而(3)得证.

下面证(1)⇒(2),设 $G=G_0\geqslant C_1\geqslant\cdots\geqslant C_r=1$ 是幂零群 G 的中心群列,设 $H<G$,取正整数 k,使得 $G_{k+1}\leqslant H$,但 $G_k\not\leqslant H$.由于 $C_r=1$,这样的 k 存在.

显然,$[G_k,H]\leqslant[G_k,G]$.取 $x\in G_k,y\in G$,由于 $G_k/G_{k+1}\leqslant Z(G/G_{k+1})$,故$[x,y]\in G_{k+1}$,从而有$[G_k,H]\leqslant H$.这就推得 $G_k\leqslant N_G(H)$.但 $G_k\not\leqslant H$,故有 $H<N_G(H)$.

(2)⇒(5),设(2)成立,H 为 G 的极大子群,由假设知 $H<N_G(H)$,故必有 $N_G(H)=G$,因而有 $H<G$.

(4)⇒(1),先证明两个幂零群的直积仍为幂零群,可得结论成立.

最后,我们决定有限交换群的结构以及小阶数的 p 群结构.

引理 2.9.9 循环p 群 P 的每个非生成元必为 P 中某元的 p 次幂.

证明 P 恰有一个由 x^p 生成的指数为 p 的子群 Q,其中 x 为 P 的生成元.若 $y\in Q$,则对整数 $n,y=(x^p)^n=(x^n)^p$.

因而Q 中每个元是 P 中某元的 p 次幂,又 Q 是 P 的唯一的极大子群,又 P 的生成元素不能属于 P 的任何一个极大子群中,故Q恰是由 P 的非生成元组成的集合.所以

P 的每个非生成元必为 P 中某元的 p 次幂.

定理 2.9.10 有限交换 p 群是循环 p 群的直积.

证明 设 P 为有限交换 p 群,对 $|P|$ 用归纳法. 设 $|P|>p$ 且结论对于阶小于 $|P|$ 的交换 p 群成立. 令 Q 是 P 的极大子群,则 $|P/Q|=p$.

由归纳假设,$Q=Q_1\times\cdots\times Q_s$,其中对 $\forall\ i$,Q_i 是 p^{a_i} 阶循环群. 不失一般性可设 $a_1\geqslant\cdots\geqslant a_s\geqslant 1$. 令 $x\in P$,但 $x\notin Q$,因为 $|P/Q|=p$,我们有 $x^p\in Q$,因而 $x^p=y_1\cdots y_s$,其中 $\forall\ i$ 来说,$y_i\in Q_i$,若对某个 i 以及某个 $x_i\in Q_i$ 有 $y_i=x_i^p$,则 $(xx_i^{-1})^p=x^px_i^{-p}=x^py_i^{-1}=y_1\cdots y_{i-1}\cdot 1\cdot y_{i+1}\cdots y_s$.

但 $xx_i^{-1}\notin Q$,由此事实可知,存在 $x\in P-Q$ 使得 $x^p=y_1\cdots y_s$,其中 y_i 或是 Q_i 的生成元,或为单位元.

若 $x^p\neq 1$,则 P 是 $\langle x\rangle$ 与 Q 的直积,因而可设 $x^p\neq 1$,在此情况下,存在某个 i 使得 $y_i\neq 1$,令 $j(1\leqslant j\leqslant s)$ 是使得 $y_i\neq 1$ 的最小整数.

我们现在有 $x^p=y_j\cdots y_s$. 因为 P 是交换的,则 x^p 的阶是 $y_j,\cdots,y_s$ 阶的最小公倍数 p^{a_j},因而 $|\langle x\rangle|=p^{a_j+1}$. 令 $\overline{Q}\leqslant P$ 是除 Q_j 以外的所有 Q_i 的直积,则

$$|\overline{Q}|=|Q|/|Q_j|=|Q|/p^{a_j}.$$

若我们能证明 $\langle x\rangle\cap\overline{Q}=1$,则 $\langle x\rangle\overline{Q}$ 就是阶为 $p|Q|=|P|$ 的循环群的直积,因而 P 是循环群的直积. 设 $x^t\in\langle x\rangle$,因 $x^p\in Q$,而对每个 $1\leqslant n<p$,$x^n\notin Q$,故仅当 $p|t$ 时才有 $x^t\in Q$. 令 $t=mp$,其中 $0\leqslant m<p^{a_j}$,于是 $x^t=(x^p)^m=y_j^m\cdots y_s^m$. 因为 $m<p^{a_j}=|\langle y_j\rangle|$,故 $y_j^m\neq 1$,这说明 x^t 在 $Q=Q_1\times\cdots\times Q_s$ 的分解式中的第 j 个分量不为 1. 又由 $\overline{Q}$ 的作法知,$\langle x\rangle\cap\overline{Q}=1$. 结论得证.

定理 2.9.11(有限交换群基本定理) 有限交换群是循环 p 群的直积.

证明 由定理 2.9.4 知,有限交换群是它的 Sylow 子群的直积. 又由定理 2.9.6 知,每一个 Sylow 子群是循环 p 群的直积. 结论得证.

定理 2.9.12 设 G 为 p^3 阶非交换群,则 G 同构于下列四种群之一:

(1) $p\neq 2$:

(i) $G=\langle x,y\mid y^{p^2}=x^p=1,x^{-1}yx=y^{1+p}\rangle\cong Z_{p^2}\times Z_p$;

(ii) $G=\langle x,y\mid x^p=y^p=z^p=1,[x,y]=z,[x,z]=[y,z]=1\rangle\cong(Z_p\times Z_p)\times Z_p$;

(2) $p=2$:

(iii) $G=\langle x,y\mid y^4=x^2=1,x^{-1}yx=y^2\rangle\cong Z_4\times Z_2$(二面体群);

(iv) $G=\langle x,y\mid x^4=1,x^2=y^2,x^{-1}yx=y^2\rangle$(四元数群).

证明 我们分两种情况讨论:$p\neq 2$ 与 $p=2$.

(1) $p\neq 2$

(i) G 含有 p^2 阶元. 我们希望证明存在 p 阶元 x,p^2 阶元 y 使得 $x\notin\langle y\rangle$. 因为在这

种情况下$\langle y\rangle \lhd G$，从而$G=\langle y\rangle\times\langle x\rangle$且$G\cong Z_p\times Z_p$. 因为$G$为$p^2$阶群，故存在$x\notin\langle y\rangle$. 若$x^p=1$，则结论得证.

设$x^p\neq 1$，则$|Z(G)|=p$且$\langle y\rangle\cap Z(G)\neq 1$. 由此得$Z(G)\leqslant\langle y\rangle$，又$Z(G)=\langle y\rangle$，

于是$|G/Z(G)|=p^2$，又$G/Z(G)$不是循环群，因而$\exp(G/Z(G))=p$.

因为$(xZ(G))^p=Z(G)$，而$x^p\neq 1$，故存在$1\leqslant k<p$，使得$x^p=y^{kp}$，用y代替y^{-k}得$x^p=y^{-p}$. 因为$\langle y\rangle=\langle y^k\rangle$，故仍有$|y|=p^2$，$x\notin\langle y\rangle$. 因为$G$是非交换的，$G/Z(G)$是交换的，故$G=Z(G)$.

特别地，$[x,y]\in Z(G)$，$(xy)^p=x^py^p[x,y]^{\frac{p(p-1)}{2}}$. 用$x$代替$xy$，我们仍有$x\notin\langle y\rangle$，于是$x$和$y$即为所求.

下证半直积的唯一性. 由$\mathrm{Aut}(Z_{p^2})$是$p(p-1)$阶的交换群，再由Sylow定理知，$\mathrm{Aut}(Z_{p^2})$恰有一个p阶子群，于是存在Z_p到$\mathrm{Aut}(Z_{p^2})$的一个单同态(可取为共轭变换)使其同态像为p阶子群，而任何两个单同态有相同的像. 由直积$Z_{p^2}\times Z_{p^2}$的唯一性，即含有p^2阶元的p^3阶群恰有一个同构类.

(ii)G没有一个p^2阶元. 从(i)的证明过程可知，G是一个p^2阶的极大子群，$H\cong Z_p\times Z_p$与不在H中的一个p阶元生成的子群$K\cong Z_p$的半直积，因而我们只需证半直积的唯一性.

由$\mathrm{Aut}(Z_p\times Z_p)\cong GL(2,p)$，当$Z_p\times Z_p=\langle x\rangle\times\langle y\rangle$时，$\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL(2,p)$对应于$\mathrm{Aut}(Z_p\times Z_p)$的自同构$\varphi: x\longmapsto x^ay^c, y\longmapsto x^by^d$，则

$$|\mathrm{Aut}(Z_p\times Z_p)|=p(p-1)^2(p+1)$$

又由Sylow定理知，$\mathrm{Aut}(Z_p\times Z_p)$中所有$p$阶子群是共轭的，令$\psi$和$\tau$是$Z_p$到$\mathrm{Aut}(Z_p\times Z_p)$的单同态(这样的单同态一定存在).

例如，令Z_p的一个生成元对应于由$\begin{pmatrix}a & b\\ c & d\end{pmatrix}$所确定的自同构$\varphi$，于是存在$f\in\mathrm{Aut}(Z_p\times Z_p)$使得$\tau(Z_p)=f\psi(Z_p)f^{-1}=(\bar{f}\cdot\psi)(Z_p)$，其中$\bar{f}$是由$f$诱导出的$\mathrm{Aut}(Z_p\times Z_p)$的自同构，我们有

$$(Z_p\times Z_p)\times_\tau Z_p\cong(Z_p\times Z_p)\times_{\bar{f}\cdot\psi}Z_p\cong(Z_p\times Z_p)\times_\psi Z_p$$

结论得证.

(2)$p=2$

(iii)由G一定有4阶元，设x和y分别为G中2阶元和4阶元使得$x\notin\langle y\rangle$. 若G中2阶元的个数不等于1，则类似于(i)的证明可知$G\cong Z_4\times_\psi Z_2\cong D_8$，其中$D_8$为二面体群，$\psi$为$Z_2$到$\mathrm{Aut}(Z_4)\cong Z_2$的唯一单同态.

(iv)设t是G唯一的2阶元，令$x,y\in G$，如(iii)所设，则$Q=\langle y\rangle\lhd G$，$G/Q=\langle xQ\rangle$.

因为$|x|\neq 2$,故有$x^2=t=y^2$.由此可见,G中每个元可唯一表示为$x^a y^b$,其中$1\leqslant a\leqslant 1$,$1\leqslant b\leqslant 3$.同时不难证明,$yx=xy^3$,

由此我们可完全决定G的任意两个元素的运算.因而若这样的群存在,则在同构意义下,它是唯一的.为证明存在性,考虑$SL(2,3)$中由元素$x=\begin{pmatrix}2&1\\1&1\end{pmatrix}$,$y=\begin{pmatrix}1&1\\1&2\end{pmatrix}$生成的子群$H$.

易验证H是一个8阶非交换群且有唯一的2阶元$x^2=\begin{pmatrix}2&0\\0&2\end{pmatrix}$.

我们已经介绍了几类重要的群:

{循环群}⊂{交换群}⊂{幂零群}⊂{超可解群}⊂{可解群}.

问题 2.9

1. 求证:$Z(N\times H)=Z(H)\times Z(N)$.
2. 设G为有限幂零群,G/G'是循环群,证明:G是循环群.
3. 设G为有限群,$P\in \mathrm{Syl}_p(G)$,证明:若$N_G(P)\subseteq H\subseteq G$,则$N_G(H)=H$.
4. 证明:G为有限幂零群$\Leftrightarrow$对$\forall\ x,y\in G$,只要$(|x|,|y|)=1$,就有$xy=yx$.
5. 证明:有限幂零群的子群和商群都是幂零群.有限幂零群的直积也是幂零群.
6. 求证:有限群G是二面体群的充要条件是G可由两个2阶元x和y生成.特别地,$G=(xy)\times(x)$.
7. 如果G是有限幂零群,且$p_1p_2\cdots p_r$是乘积等于G的阶的任意地排列的素数,则G具有合成群列$G=G_0\geqslant G_1\geqslant\cdots\geqslant G_r=1$,这里$G_{i-1}/G_i$的阶是$p_i$.

§2.10 群的构造

群论研究可以分成两个方面,一方面是对给定的有背景的重要群,如各种对象的对称群、置换群、矩阵群(与几何、物理的联系)、有限单群、可解群(与解代数方程有联系)等等,讨论群的结构,以及它与其他群的关系(群的表示问题),另一方面是尽可能多地构造出一些新的群来,或者是借助于已知群去构造新群,或者就是根据需要去构造新群.常称前者为群的结构理论和表示理论,而称后者为群的构造理论.

前面讨论过的子群、商群,都是从一个已知群获得新群的方法.

例如,从一般线性群$GL_n(F)$得到其子群$SL_n(F)$,以及从$SL_n(F)$得到$PSL_n(F)$等等.

由两个已知群K和H,可以构造一个新的群,即它们的外直积$H\times K$.由已知的两

个群 H 和 K，还可用别的方法构造新群吗？

一个我们非常感兴趣的问题是：能否构造一个群 G，它以 H 为正规子群（即它有一个正规子群与 H 同构），而它关于 H 的商群 $G/H\cong K$，即所谓群 H 借助于群 K 的扩张问题. 这个问题的重要性我们已在有限群的讨论中看到过了. 下面我们来构造自由群.

著名的 Cayley 定理说：一个 n 阶有限群可以看作 n 元对称群 S_n 的一个子群. 与此对偶地我们可以问：是否可找到一个群 G，使得某一类群中的所有群都是这个群 G 的同态像？

如果这样的群 G 存在，那么研究这类群就归结为研究群 G 的商群，这就与研究有限群就是研究群 S_n 的子群相当了. 在前面曾说过，如果有满同态 $G\to G'$，则群 G 中的一些关系式必传递给 G'，这样上面我们想找的那个群 G，必是相当"自由"的群，即是关系很少的群.

这样的群我们已见过，加群 Z 和循环群之间就有这种关系：任一循环群都是群 Z 的同态像. 下面首先来推广这一结果.

定理 2.10.1　任意由 n 个元素生成的交换群 G 都是 Z^n 的同态像.

证明　首先证明 Z^n 中每个元素可以唯一表示成 $m_1e_1+\cdots+m_ne_n, m_i\in Z$ 的形式. 任取 $a\in Z^n$，则

$$a=(m_1,m_2,\cdots,m_n)=(m_1,0,\cdots,0)+(0,m_2,0,\cdots,0)+\cdots+(0,\cdots,0,m_n)=m_1e_1+\cdots+m_ne_n.$$

即 a 可表成上面的形式. 若 $r_1e_1+\cdots+r_ne_n=m_1e_1+\cdots+m_ne_n$，则有

$$(0,\cdots,0)=(r_1-m_1)e_1+\cdots+(r_n-m_n)e_n=(r_1-m_1,\cdots,r_n-m_n)$$

即在群 Z 中有 $r_i-m_i=0$，即 $r_i=m_i, i=1,2,\cdots,n$，即证得表示形式的唯一性.

再看由 n 个元素 $g_1,\cdots,g_n$ 生成的交换群 G（其运算也记作＋），这时 G 的每一个元素 g 都可表成某些 $g_i(i=1,\cdots,n)$ 的和. 注意到 G 是交换群，我们可以把同一脚标的 g_i，$-g_i$ 调换到一起，这样就有

$$a=m_1g_1+\cdots+m_ng_n, m_i\in Z$$

规定

$$\varphi: Z^n\to G, m_1e_1+\cdots+m_ne_n\longmapsto m_1g_1+\cdots+m_ng_n,$$

由于上面形式的存在性和唯一性，得 φ 是一个映射，且是满射. 容易验证，φ 是保持运算的，则 φ 是 Z^n 到 G 上的同态映射.

定义 2.10.1　称群 Z^n 为 n 阶自由交换群.

现在我们进一步研究某些群的结构，首先介绍约束条件最少的群——自由群以及用定义关系刻画群结构的方法.

定义 2.10.2 设 S 为任意集合，S 中有限个元素 $x_1,x_2,\cdots,x_n$ 连在一起叫做是一个字. 字 $x_1x_2\cdots x_n$ 和 $y_1y_2\cdots y_m$ 相等，如果 $n=m$ 且 $x_i=y_i,1\leqslant i\leqslant n$.

以 $\Sigma^*(S)$表示所有这样的字(包括空字 1)组成的集合，在 $\Sigma^*(S)$中定义两个字的运算为：

$$(x_1x_2\cdots x_n)(y_1y_2\cdots y_m)=x_1\cdots x_ny_1\cdots y_m,$$

对每个字 $a\in\Sigma^*(S)$规定 $1a=a1=a$，则这个运算显然满足结合律，从而 $\Sigma^*(S)$对上述运算形成一个幺半群，称为集合 S 上的自由幺半群.

集合 S 叫做$\Sigma^*(S)$的基."自由"一词意味着 $\Sigma^*(S)$中除了含幺半群定义中的要求之外，没有任何其他拘束条件.

如果将自由含幺半群 $\Sigma^*(S)$扩大成群，$\forall\ x\in S$ 应当有逆元素，所以给了集合 S 之后，再考虑集合 $S^{-1}=\{x^{-1}\mid x\in S\}$. 令

$$F(S)=\{a_1a_2\cdots a_n\mid a_i\in S\cup S^{-1},1\leqslant i\leqslant n\},$$

这里当 $n=0$ 时，规定 $a_1\cdots a_n=1$，$F(S)$中运算仍定义为

$$(a_1\cdots a_n)(b_1\cdots b_m)=a_1\cdots a_nb_1\cdots b_m,$$

但是约定 $aa^{-1}=a^{-1}a=1$，对$\forall\ a\in F(S)$，$1\cdot a=a\cdot 1=a$. 例如$(ab)(b^{-1}c)=ac$，$(ab)(b^{-1}a^{-1})=1$ 等等. 这时，$F(S)$中每个元素均有逆元素，例如 a^{-1}的逆元素为 a，$(a^3b^{-1}c)^{-1}=c^{-1}ba^{-3}$. $F(S)$对于上述运算和约定成群，叫做集合S 上的自由群，S 叫做此自由群的基. 显然 S 是群 $F(S)$的一个生成元系.

定义 2.10.3 如果 S 是有限集，则 $F(S)$叫做有限生成自由群.

特别地，当 $S=\{a\}$时，$F(S)=\langle a\rangle=\{a^n\mid n\in Z\}$就是无限循环群，而当$|S|\geqslant 2$ 时，$F(S)$是无限非 Abel 群.

定理 2.10.2 每个群都是自由群的商群. 每个有限生成群都是有限生成自由群的商群.

证明 设 G 为群. 取 G 的一个生成元系 Σ(例如可取 $\Sigma=G$)，定义集合 $S=\{X_a\mid a\in\Sigma\}$，并考虑映射 $f:F(S)\to G$，其中 $f(X_a)=a,f(X_a{}^{-1})=a^{-1}$.

然后对于 $A_i\in\Sigma\cup\Sigma^{-1}(1\leqslant i\leqslant n)$，定义：

$$f(A_1\cdots A_n)=f(A_1)\cdots f(A_n).$$

这个映射是可以定义的，即不依赖于 $F(S)$中元素的不同表达方式，因为不同表达方式是由于插入或消去 $X_aX_a{}^{-1}$或 $X_a{}^{-1}X_a$ 造成的，而

$$f(X_aX_a{}^{-1})=aa^{-1}=1,f(X_a{}^{-1}X_a)=a^{-1}a=1.$$

进一步易知 f 是群同态，并且是满的，因为对每个生成元 $a\in\Sigma,a=f(X_a)\in\mathrm{Im}f$，从而 $G=\langle\Sigma\rangle=\mathrm{Im}f$. 根据同态基本定理，$G\cong F(S)/\mathrm{Ker}f$，即 G 同构于自由群 $F(S)$的商群. 如果 G 是有限生成的，令有限集 Σ 是 G 的一个生成元系，则 $S=\{X_a\mid a\in\Sigma\}$也是

有限集,从而 $F(S)$ 为有限生成自由群.

设 G 同构于自由群 $F(S)$ 的商群,$f: F(S)/K \cong G$,K 是 $F(S)$ 的正规子群,则 G 是由 $f(S)=\Sigma$ 生成的,进一步,对 K 中每个元素 α,G 中就有一个等式 $f(\alpha)=1_G$,K 中有多少元素,G 中就相应有多少个关系.如果 P 是 K 的一个子集,且 K 是 $F(S)$ 中包含 P 的最小正规子群(叫做由 P 生成的正规子群),则 K 中每个元素均可由 P 在 $F(S)$ 中的全部共轭集合的元素运算出来,反映在群 G 中,G 的所有关系均可由 P 中元素给出的关系推导出来.

定义 2.10.4 我们把由 P 中元素给出的那些关系全体叫做群 G 的定义关系集,并且群 G 写成 $G=\langle \Sigma \mid f(\alpha)=1, \forall\ \alpha\in P\rangle$,这种刻画群的方式为群 G 的一个表现.

例如令 $S=\{a,b\}$,K 是 $F(S)$ 中的元素 a^3 和 $(ab)^2$ 生成的正规子群,如果 $G\cong F(S)/K$,则 G 的结构可以写成 $G=\langle A,B \mid A^3=(AB)^2=1\rangle$.

例 2.10.1 以 φ 表示关系集合为空集.$G=\langle S\mid\varphi\rangle$ 即是以 S 为基的自由群,因为此时 $K=\{1\}$,$G\cong F(S)/\{1\}=F(S)$.

例 2.10.2 $Z_n\cong\langle a\rangle/\langle a^n\rangle=F(S)/\langle a^n\rangle$,其中 $S=\{a\}$,因而 n 阶循环群的表现为 $Z_n=\langle a\mid a^n=1\rangle$.

例 2.10.3 正 $n(n\geqslant 3)$ 边形对称群 D_n 是 $2n$ 阶群,它有生成元 $\langle\sigma,\tau\rangle$,其中 $\sigma^n=\tau^n=1$,$(\tau\sigma)^2=1$.令 F 是以 $\{a,b\}$ 为基的自由群,则有群的满同态 $f: F\to D_n$,$f(a)=\sigma$,$f(b)=\tau$,由同态基本定理可知 $D_n\cong F/\mathrm{Ker}f$.

由于 $f(a^n)=\sigma^n=1$,$f(b^2)=\tau^2=1$,$f((ba)^2)=(\tau\sigma)^2=1$,$a^n,b^2,(ba)^2\in\mathrm{Ker}f$.令 K 是 F 中由 $a^n,b^2,(ba)^2$ 生成的正规子群,则 $K\leqslant\mathrm{Ker}f$.

现在考虑商群 F/K.以 A 和 B 分别表示 a 和 b 在 F/K 中的象,则 $A^n=B^2=(BA)^2=1$,F/K 可由 $\{A,B\}$ 生成,由于 $BA=A^{-1}B^{-1}=A^{n-1}B$,F/K 中元素可表示成 $A^iB^j(0\leqslant i\leqslant n-1, 0\leqslant j)$,从而 $|F/K|\leqslant 2n$.

$$2n=|D_n|=|F/\mathrm{Ker}f|=|F/K|/|\mathrm{Ker}f/K|\leqslant 2n/|\mathrm{Ker}f/K|$$

因此,$K=\mathrm{Ker}f$,$D_n\cong F/K$,于是 D_n 有如下的表现:

$$D_n=\langle a,b\mid a^n=b^2=(ba)^2=1\rangle$$

例 2.10.4 令 $Q_8=\langle a,b\mid a^4=1,b^2=a^2,ba=a^3b\rangle$.$Q_8$ 中每个元素均可写成 $a^ib^j(0\leqslant i\leqslant 3, 0\leqslant j\leqslant 1)$,从而 $|Q_8|\leqslant 8$.我们有一个具体矩阵群 $G=\langle A,B\rangle$,其中

$$A=\begin{pmatrix}0&1\\-1&0\end{pmatrix},B=\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix}\quad(\mathrm{i}=\sqrt{-1}),$$

满足 $A^4=1$,$B^2=A^2$,$BA=A^3B$.

并且可直接验证 $A^iB^j(0\leqslant i\leqslant 3, 0\leqslant j\leqslant 1)$ 为 8 个不同的矩阵,因此 $|G|=8$.然后可按例 2.10.3 的方法得出 $G\cong Q_8$,即 Q_8 为 8 阶非 Abel 群.

定义 2.10.5 设 S 为任意集合，表现为 $F=\langle S\mid ba=ab,\forall\ a,b\in S\rangle$ 的群叫做以 S 为基(或在 S 上)的自由 Abel 群.

由于元素可交换，所以 F 中元素均可写成

$$g=a_1^{n_1}a_2^{n_2}\cdots a_r^{n_r}(r\geqslant 0,n_i\in Z,n_i\neq 0,a_i\in S,1\leqslant i\leqslant r)$$

其中 $a_1,a_2,\cdots,a_r$ 是 S 中不同元素，并且若不考虑前后次序，g 的这个表达方式是唯一的. 可以像定理 2.10.1 那样证明每个(有限生成)Abel 群均是(有限生成)自由 Abel 群的商群. 为了进一步看清有限生成自由 Abel 群的结构，我们现在引进群的直积.

定义 2.10.6 设 $G_1,\cdots,G_n$ 是群，在集合的直积

$$G=G_1\times\cdots\times G_n=\{(g_1,\cdots,g_n)\mid g_i\in G_i,1\leqslant i\leqslant n\}$$

中定义运算

$$(g_1,\cdots,g_n)(g'_1,\cdots,g'_n)=(g_1g'_1,\cdots,g_ng'_n),$$

易证 G 对此运算成群，叫做群 $G_1,\cdots,G_n$ 的直积.
它的幺元素为 $(1_{G_1},\cdots,1_{G_n})$，元素 $(g_1,\cdots,g_n)$ 的逆为 $(g_1^{-1},\cdots,g_n^{-1})$.

设 G 和 K 是群，则 $G\times 1=\{(g,1)\mid g\in G\}$ 和 $1\times K=\{(1,k)\mid k\in K\}$ 是 $G\times K$ 的两个子群，并且 $G\times 1\cong G,1\times K\cong K$. $G\times 1$ 中元素和 $1\times K$ 中元素可交换，$G\times K=(G\times 1)(1\times K)$，$(G\times 1)\cap(1\times K)=\{1\}$.

引理 2.10.3 设 $H,K\leqslant G,H\cap K=\{1\},G=HK$，且对每个 $h\in H,k\in K,hk=kh$，则 $G\cong H\times K$.

证明 由 $G=HK$ 和 H 中元素与 K 中元素的交换性，可知 G 中每个元素均可表成 $g=hk,h\in H,k\in K$. 再由 $H\cap K=\{1\}$，g 的这个表达式是唯一的. 于是我们可以定义 $f:G\to H\times K,hk\mapsto(h,k)$.

由上知这是一一对应，并且 $f((hk)(h'k'))=f(hh',kk')=(hh',kk')=f(hk,h'k')$，从而 f 为同构，即 $G\cong H\times K$.

下面定理是判别一个群为某些子群直积的方法.

以后将 $G=G_1\times\cdots\times G_n$ 中元素 $(g_1,1,\cdots,1)$ 等同于 G_1 中元素 g_1，由此将 G_1 看成是 G 的正规子群. 类似地，$G_2,\cdots,G_n$ 也自然地看成 G 的正规子群，从而 G 的每个元素唯一地表成 $g=g_1\cdots g_n(g_i\in G_i)$.

定理 2.10.4 设 $G_1,\cdots,G_n$ 是 G 的正规子群，$n\geqslant 2$，则以下三条件是彼此等价的：

(1) $G=G_1\times\cdots\times G_n$；

(2) G 中每个元素可以唯一表示成 $g=g_1\cdots g_n$ 其中 $g_i\in G_i$；

(3) $G=G_1\cdots G_n$，且对每个 $m,1<m\leqslant n,(G_1G_2\cdots G_{m-1})\cap G_m=\{1\}$.

证明 (1)⇒(2)，如定理前面的约定，G 中元素 $(g_1,\cdots,g_n)$ 唯一地写成

$$(g_1,1,\cdots,1)\cdots(1,\cdots,1,g_n)=g_1\cdots g_n.$$

(2)⇒(3) 设 $g\in(G_1\cdots G_{m-1})\cap G_m$，则有 $g_i\in G_i$ 使得 $g=g_1\cdots g_{m-1}=g_m$，于是 $1=g_1\cdots g_{m-1}g_m^{-1}$，由(2)中唯一性假设，$g_m{}^{-1}=1$，从而 $g=g_m=1$，即

$$(G_1\cdots G_{m-1})\cap G_m=\{1\}.$$

(3)⇒(1). 令 $J_m=G_1\cdots G_m$. 由 G_i 是 G 的正规子群 $(1\leqslant i\leqslant n)$，$J_m$ 是 G 的正规子群. 现在对 m 归纳证明 $J_m=G_1\times\cdots\times G_m(2\leqslant m\leqslant n)$.

当 $m=2$ 时，$\forall\ g_1\in G_1, g_2\in G_2$，

$$g_1g_2g_1^{-1}g_2^{-1}=g_1(g_2g_1^{-1}g_2^{-1})=(g_1g_2g_1^{-1})g_2^{-1}\in G\cap G_2=\{1\}, g_1g_2=g_2g_1,$$

由引理 2.10.1，$J_2=G_1\times G_2$. 现在设 $J_{m-1}=G_1\times\cdots\times G_{m-1}$，则 J_{m-1}, G_m 是 G 的正规子群，$J_m=J_{m-1}G_m$，且由(3)中假设 $J_{m-1}\cap G_m=\{1\}$，于是由定理 2.10.1 知，

$$J_m=J_{m-1}\times G_m=G_1\times\cdots\times G_m.$$

特别当 $m=n$ 时，$G=J_n=G_1\times\cdots\times G_n$.

现在回到有限生成自由 Abel 群 G. 设它的基为 $S=\{a_1,\cdots,a_r\}$，则 G 中每个元素唯一表示成 $g=a_1^{\lambda_1},\cdots a_r^{\lambda_r}, \lambda_i\in\mathbf{Z}$，由于 Abel 群 G 的子群 $G_i=\langle a_i\rangle$ 均是正规的，从定理 2.10.2 的(2)即知 $G=G_1\times\cdots\times G_r$. 但是 $G=\langle a_i\rangle$ 是无限循环群，G 同构于 r 个无限循环群的直积.

对于群 G，把 n 个群 G 的直积写成 G^n，而令 $G_n=\{g^n\mid g\in G\}$. 当 G 为 Abel 群时，G_n 是 G 的子群. 现在设 G 是有限生成自由 Abel 群，则

$$G=\langle a_1\rangle\times\cdots\times\langle a_r\rangle\cong Z^r,$$

其中 $\langle a_i\rangle$ 均是无限循环群.

对每个 $n\geqslant 2$，$G_n=\langle a_1^n\rangle\times\cdots\times\langle a_r^n\rangle$，

$$G/G_n\cong(\langle a_1\rangle/\langle a_1^n\rangle\times\cdots\times(\langle a_r\rangle/\langle a_r^n\rangle)\cong Z_n\times\cdots\times Z_n=Z_n^r,$$

$$|G/G_n|=|Z_n^r|=n^r,$$

因此数 $r=\log|G/G_n|/\log n$ 是由群 G 本身所唯一决定的. 换句话说，如果 $G\cong Z^r$ 且又 $G\cong Z^s$，则 $r=s$，所以，有限生成自由 Abel 群本质上是 $Z^r(r=1,2,\cdots)$，并且它们互不同构.

定义 2.10.7　如果 $G\cong Z^r$，r 称为有限生成自由 Abel 群 G 的秩，记为 rank(G).

综合上述，我们证明了下面的结构定理.

定理 2.10.5　有限生成自由 Abel 群 G 同构于有限个无限循环群的直积，$G\cong Z^r$，$r=\text{rank}(G)\geqslant 1$.

两个这样的群 G 和 G' 同构 ⇔ rank$(G)=$ rank(G').

推论 2.10.6　设 S 和 S' 是有限生成自由 Abel 群 G 的两组基，则 $|S|=|S'|$.

问题 2.10

1. 令 $G=\langle g_1,g_2,\cdots,g_n\rangle$ 由 2 个元素生成，如果 G 的子群 A 具有有限指数，则 A 可

以由 $2n[G:A]$ 个元素生成.

2. 若 $n\geqslant 3$,试问 $A_n\times Z_2$ 与 S_n 是否同构?

3. 设 G_1,G_2,G_3 为群,则

1)$G_1\times G_2\cong G_2\times G_1$;

2)$(G_1\times G_2)\times G_3\cong G_1\times(G_2\times G_3)$.

4. 如果 n 为正整数,求证:$D_{2n}\cong D_n\times Z_2$.

5. 设 G_1 和 G_2 是非交换单群,则 $G_1\times G_2$ 的非平凡正规子群只有 G_1 和 G_2.

6. 设 $G_i(1\leqslant i\leqslant N)$ 为群,则

1)$C(G_1\times G_2\times\cdots\times G_n)=C(G_1)\times C(G_2)\times\cdots\times C(G_n)$;

2)$G_1\times G_2\times\cdots\times G_n$ 为 Abel 群当且仅当每个 G 均为 Abel 群.

7. 设 $G_i(1\leqslant i\leqslant n)$ 为群,$N_i\leqslant G_i$,则

1)$N_1\times N_2\times\cdots\times N_n\leqslant G_1\times G_2\times\cdots\times G_n$;

2)$N_1\times N_2\times\cdots\times N_n\lhd G_1\times G_2\times\cdots\times G_n\Leftrightarrow\forall\, i,N_i\lhd G_i$;

3)当 $N_1\times\cdots\times N_n$ 是 $G_1\times\cdots\times G_n$ 的正规子群时,

$G_1\times\cdots\times G_n/N_1\times\cdots\times N_n\cong G_1/N_1\times\cdots\times G_n/N_n$.

8. 试证:$5\times 7\times 3$ 阶群一定是循环群.

9. 令 $G=G_1\times G_2$,$H\lhd G$ 且 $H\cap G_i=1$,$i=1,2$. 试证:H 是 Abel 群.

10. 设 $n_1,n_2,\cdots,n_r$ 为自然数,则

1)$Z_{n_1}\times Z_{n_2}\cong Z_n\ln_2\Leftrightarrow(n_1,n_2)=1$;

2)如果 $n_1,n_2,\cdots,n_r$ 两两互素,则 $Z_{n1}\times Z_{n2}\times\cdots\times Z_{nr}\cong Z_{n_1n_2\cdots n_r}$.

§2.11 交换群的结构

在本节中,我们把 Abel 群 A 中运算写成加法,幺元素为 0,元素 a 的逆是 $-a$,n 个 a 运算为 $a+a+\cdots+a=na$,有限阶元素 a 的阶为满足 $na=0$ 的最小正整数 n. $nA=\{na\mid a\in A\}$,直积则改叫做直和并且写成 $A\oplus A'$,n 个 A 的直和仍表成 A^n.

定理 2.11.1 有限生成自由 Abel 群 F 的每个子群 $G(G\neq\{0\})$ 仍是有限生成自由 Abel 群,且 $\mathrm{rank}(G)\leqslant\mathrm{rank}(F)$.

证明 当 $n=1$ 时,由无限循环群的子群特性可知定理 2.11.1 成立. 现在假设定理对于秩小于 n 的所有自由 Abel 群均成立. 以 S 表示集合 $\{s\in\mathbf{Z}\mid$ 存在 F 的一组基 $\{y_1,\cdots,y_n\}$,使得 G 中有形如 $sy_1+k_2y_2+\cdots+k_ny_n(k_i\in\mathbf{Z})$ 的元素$\}$,注意 $\{y_2,y_1,\cdots,y_n\}$ 也是 F 的一组基,从而 $k_2\in S$. 类似地,对于每个 $k_i\in S$,由于 $G\neq\{0\}$,S 中有非零整数. 易知若 $s\in S$,则 $-s\in S$,因此 S 中有非零正整数. 以 d_1 表示 S 中的最小正整数,于是存在 v

$=d_1y_1+k_2y_2+\cdots+k_ny_n\in G$.

令 $k_i=d_1q_i+r_i(0\leqslant r<d_i)$，则

$$v=d_1(y_1+q_2y_2+\cdots+q_ny_n)+r_2y_2+\cdots+r_ny_n).$$

令 $x_1=y_1+q_2y_2+\cdots+q_ny_n$，$\{x_1,y_2,\cdots,y_n\}$ 也是 F 的一组基，从而 $r_i\in S$，由 d_1 的极小性知 $r_i=0(2\leqslant i\leqslant n)$. 因此 $v=d_1x_1\in G$. 令 $H=\langle y_2,\cdots,y_n\rangle$，这是秩为 $n-1$ 的自由 Abel 群.

我们现在证明 $G=\langle v\rangle\oplus(G\cap H)=\langle d_1x_1\rangle\oplus(G\cap H)$.

首先，由于 $\{x_1,y_2,\cdots,y_n\}$ 为 F 的基，$\langle v\rangle\cap(G\cap H)=\{0\}$. 其次对每个元素 $u=t_1x_1+t_2y_2+\cdots+t_ny_n\in G(t_i\in\mathbf{Z})$.

令

$$t_i=d_1q_1+r_1,0\leqslant r_1<d_1,u-q_1v=r_1x_1+t_2y_2+\cdots+t_ny_n\in G,$$

由 d_1 的极小性知 $r_1=0$，于是

$$t_2y_2+\cdots+t_ny_n\in G\cap H,u=q_1v+(t_2y_2+\cdots+t_ny_n)\in\langle v\rangle+(G\cap H),$$

因此 $G=\langle d_1x_1\rangle\oplus(G\cap H)$.

如果 $G\cap H=\{0\}$，则 $G=\langle d_1x_1\rangle$，定理成立.

如果 $G\cap H\neq\{0\}$，则 $G\cap H$ 是秩为 $n-1$ 的自由 Abel 群 H 的子群，根据归纳假设存在 H 的一组基 $\{x_2,\cdots,x_n\}$，正数 $r,d_2,\cdots,d_r$ 使得 $d_2|d_3|\cdots|d_r$，且 $GH=\langle d_2x_2\rangle\oplus\cdots\oplus\langle d_rx_r\rangle$，于是

$$F=\langle x_1\rangle\oplus\cdots\oplus\langle x_r\rangle,G=\langle d_1x_1\rangle\oplus\cdots\oplus\langle d_rx_r\rangle.$$

令 $d_2=qd_1+r,0\leqslant r<d_1$，则 $\{x_2,x_1+qx_2,x_3,\cdots,x_n\}$ 为 F 的基，而

$$rx_2+d_1(x_1+qx_2)=d_1x_1+d_2x_2\in G,$$

则 $r\in S$，由 d_1 的极小性知 $r=0$，即 $d_1|d_2$.

定理 2.11.2 有限生成 Abel 群 A 均同构于 $Z^r\oplus Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，其中 $r,t\geqslant 0,1<m_1\leqslant\cdots\leqslant m_t$ 且 $m_1|m_2|\cdots|m_t$.

证明 不妨设 $A\neq\{0\}$，且 A 是由 n 个元素生成的. 于是 A 同构于秩为 n 的自由 Abel 群 F 的商群：$A\cong F/K$. 如果 $K=\{0\}$，则 $A\cong F$，从而为 $r=n,t=0$ 的情形. 如果 F 的子群 $K\neq\{0\}$，由定理 2.11.1 知存在 $x_1,\cdots,x_n\in F,d_1,\cdots,d_s\in Z,d_1|d_2|\cdots|d_s$，使得

$$F=\langle x_1\rangle\oplus\cdots\oplus\langle x_n\rangle,K=\langle d_1x_1\rangle\oplus\cdots\oplus\langle d_sx_s\rangle.$$

令 $d_{s+1}=\cdots=d_n=0$，我们有

$$\begin{aligned}G&\cong F/K\cong(\langle x_1\rangle/\langle d_1x_1\rangle)\oplus\cdots\oplus(\langle x_n\rangle/\langle d_nx_n\rangle)\\&\cong(\langle x_1\rangle/\langle d_1x_1\rangle)\oplus\cdots\oplus(\langle x_s\rangle/\langle d_sx_s\rangle)\oplus Z^{n-s}\end{aligned}$$

注意：$\langle x\rangle/\langle x\rangle=\{0\}$，以 $m_1,\cdots,m_t$ 表示 $d_1,\cdots,d_s$ 中不为 1 的那些数，则

$$G\cong Z^r\oplus Z_{m_1}\oplus\cdots\oplus Z_{m_t}，其中 r=n-s，且 m_1|m_2|\cdots|m_t.$$

设 A 是有限生成 Abel 群，以 A_t 表示 A 中有限阶元素全体. 如果 a 和 b 分别是 A 中阶数为 r 和 s 的元素，则 a^{-1} 和 ab 的阶分别是 r 和 $[r,s]$（r 和 s 的最小公倍数）. 从而 A_t 是 A 的子群，叫做 A 的扭子群. 易知 A_t 是有限 Abel 群.

定理 2.11.3　设 A 和 B 是有限生成 Abel 群，

(1)存在 A 的有限生成自由 Abel 子群 A_f，使得 $A=A_f\oplus A_t$；

(2)如果 $A=A_f\oplus A_t$，$B=B_f\oplus B_t$，其中 A_f 和 B_f 分别为 A 和 B 的有限生成自由 Abel 子群，则 $A\cong B\Leftrightarrow \mathrm{rank}A_f=\mathrm{rank}B_f$ 且 $A_t\cong B_t$.

证明　(1)根据定理 2.11.2，存在同构 $\varphi: A\cong Z_f^r\oplus T$，其中

$$T=Z_{m_1}\oplus\cdots\oplus Z_{m_t},\ 1<m_1\mid m_2\mid\cdots\mid m_t.$$

不难看出 $Z^r\oplus T$ 的扭子群就是 T，因此 $\varphi^{-1}(T)$ 就是 A 的扭子群 A_t，记 $A_f=\varphi^{-1}(Z^r)$，则 $A_f\cong Z^r$ 且 $A=A_f\oplus A_t$.

(2)如果 $A\cong B$，则 $A_t\cong B_t$，从而 $A_f\cong A/A_t\cong B/B_t\cong B_f$，于是 $\mathrm{rank}A_f=\mathrm{rank}B_f$.

反之，若 $\mathrm{rank}A_f=\mathrm{rank}B_f$，则 $A_f\cong B_f$. 如果又有 $A_t\cong B_t$，则 $A=A_f\oplus A_t\cong B_f\oplus B_t=B$.

每个有限生成 Abel 群 A 均同构于 $Z^r\oplus A_t$，其中 r 是由 A 唯一决定的，叫做 A 的秩，记为 $\mathrm{rank}A$. 当 A 为有限生成自由 Abel 群时 $A_t=\{0\}$，可知这里秩的定义与对自由 Abel 群情形的定义是一致的.

定理 2.11.4　设 A 为有限 Abel 群，$A\neq\{0\}$.

(1)存在 $1<m_1\mid m_2\mid\cdots\mid m_t(t\geqslant 1)$，使得 $A\cong Z_{m_1}\oplus\cdots\oplus Z_{mt}(m_1,\cdots,m_t)$，由 A 唯一确定；

(2)存在一组正整数 $\{p_1^{s_1},p_2^{s_2},\cdots,p_k^{s_k}\}$，$p_1,\cdots,p_k$ 为素数，$s_1,\cdots,s_k$ 为正整数，使得 $A\cong Z_{p_1^{s_1}}\oplus\cdots\oplus Z_{p_k^{s_k}}$，且集合 $\{p_1^{s_1},p_2^{s_2},\cdots,p_k^{s_k}\}$ 由群 A 唯一决定.

证明　有限 Abel 群当然是有限生成的，由定理 2.11.2 有 $Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，$f$ 中元素除 0 外均为无限阶元素，而有限群 A 中元素均为有限阶的，因此 $r=0$，

$$A\cong Z_{m_1}\oplus\cdots\oplus Z_{m_t},$$

从而得到(1)中的分解式. 令 $m_1=p_1^{\lambda_1}\cdots p_l^{\lambda_l}$，其中 $p_1,\cdots,p_l$ 是不同的素数，λ_i 为正整数，则 $Z_{m_1}\cong Z_{p_1^{\lambda_1}}\oplus\cdots\oplus Z_{p_l^{\lambda_l}}$，将 $Z_{m_1},\cdots,Z_{m_t}$ 也如此作成一些素数幂阶的循环群的直和，便得到(2)中的分解式. 下面再证满足定理条件的 $\{m_1,\cdots,m_t\}$ 和 $\{p_1^{s_1},\cdots,p_k^{s_k}\}$ 的唯一性.

先证 $\{p_1^{s_1},\cdots,p_k^{s_k}\}$ 的唯一性，对于每个素数 p，有限群 G 的 Sylow$p$-群是彼此共轭的，并且 G 中每个阶为 p 方幂的元素均在 G 的某个 Sylow$p$-群之中. 当 G 为有限 Abel$l$ 群时，每个子群均只与自己共轭，从而对 $|G|$ 每个素因子 p，G 只有唯一的一个 Sylow$p$-子群 G，并且 G_p 就是 G 中全部 p 方幂阶元素所构成的子群. 设 $|G|$ 的素因子分解式 $G=p_1^{\lambda_1},\cdots p_s^{\lambda_s}$，则 $G=G_{p_1}\oplus\cdots\oplus G_{p_s}$，即每个有限 Abel 群是它的所有 Sylow 子群的直和.

为了对有限 Abel 群 A 证明$\{p_1^{s_1},\cdots,p_k^{s_k}\}$的唯一性，我们只需对它的每个 Sylow 子群 A_p 证明即可. 以下设 A 为有限 Abel 群，即 A 的阶为 p 方幂，这时 $A\cong Z_{p^{a_1}}\oplus\cdots\oplus Z_{p^{a_r}}$.

下面证明$\{a_1,\cdots,a_r\}$的唯一性.

不妨设 $1\leqslant a_1\leqslant\cdots\leqslant a_r$. 若又有 $A\cong Z_{p^{c_1}}\oplus\cdots\oplus Z_{p^{c_d}}$，$1\leqslant c_1\leqslant c_d$ 则 $pA=pZ_{p^{a_1}}\oplus\cdots\oplus pZ_{p^{a_r}}$，于是 $A/pA\cong(Z_{p^{a_1}}/pZ_{p^{a_1}})\oplus\cdots\oplus(Z_{p^{a_r}}/pZ_{p^{a_r}})$.

但是 $Z_{p^a}/pZ_{p^a}\cong Z_p$，因此 $A/pA\cong Z_p^r$，从而$|A/pA|=p^r$.

类似地由 $A\cong Z_pc^1\oplus\cdots\oplus Z_pc_d$ 得到$|A/pA|=p^d$，我们首先得出 $r=d$.

假设 $a_1=c_1,\cdots,a_{i-1}=c_{i-1}$，而 $a_i<c_i$，则由 $m_1|m_2|\cdots|m_t$ 可知 $0\leqslant a_{1j}\leqslant a_{2j}\leqslant\cdots\leqslant a_{ij}$ $(1\leqslant j\leqslant r)$. 于是 Z_{m_i} 的 Sylowp_j-子群为 $Z_{p_j}^{a_{ij}}$. 又

$$p^{a_i}A\cong p^{a_i}Z_{p^{a_1}}\oplus\cdots\oplus p^{a_i}Z_{p^{a_r}}\cong Z_{p^{a_{i+1}-a_i}}\oplus\cdots\oplus Z_{p^{a_r-a_i}},$$

同样有

$$p^aA\cong Z_{p^{c_i-a_i}}\oplus\cdots\oplus Z_{p^{c_r-a_i}},\ p^{a_i}A/p^{a_i+1}A\cong Z_p^{\,r-i+1}.$$

$(c-a,\cdots,c_r-a$ 均为正整数)但是 $a_{i+1}-a_i,\cdots,a_r-a_i$ 中共有 $r-i$ 个数，于是 $p^{a_i}A/p^{a_i+1}A$ 又同构于不超过 $r-i$ 个 Z_p 的直和，矛盾，从而 $a_i=c_i$，$1\leqslant i\leqslant r$.

最后证明$\{m_1,\cdots,m_i\}$的唯一性. 设 $p_1,\cdots,p_r$ 是$|A|=m_1,\cdots,m_i$ 的全部素因子. 令 $m_i=p_1^{a_{i1}}\cdots p_r^{a_{ir}}\geqslant 0$，$A=Z_{m_1}\oplus\cdots\oplus Z_{mt}$的 Sylow$p_j$-子群 A_{pj}为

$$Z_{pj}^{a_{1ij}}\oplus\cdots\oplus Z_{pj}^{a_{ij}}(0\leqslant a_{1j}\leqslant\cdots\leqslant a_{ij}).$$

由上一段已知 a_{1j}，$\cdots$，a_{ij}中不为 0 的那些由$_{pj}$唯一决定，因此由 A 唯一决定. 由条件 $m_i>1$ 可知 t 和所有的 a_{ij}均由 A 唯一决定. 因此$\{m_1,\cdots,m_t\}$由 A 唯一决定，这就完成了定理的证明.

定理 2.11.4 中的$\{m_1,\cdots,m_t\}$叫做 A 的不变因子，$\{p_1^{s_1},\cdots,p_k^{s_k}\}$叫做 A 的初等因子. 对于有限生成 Abel 群 A，A 的不变因子和初等因子也分别叫做 A 的不变因子和初等因子. 综上我们得到了有限生成 Abel 群的结构定理.

定理 2.11.5　两个有限生成 Abel 群同构⇔它们有相同的秩和初等因子⇔它们有相同的秩和不变因子.

特别地，两个有限 Abel 群同构⇔有相同的初等因子⇔有相同的不变因子.

问题 2.11

1. 设 G 是由元素 a,b 生成的群，其中 a,b 的定义关系为 $a^3=b^3=e$ 和$(ab)^3=e$，写出元素并证明 G 与交代群 A_4 同构.

2. 设 G 是由元素 a,b 生成的群，其中 a,b 的定义关系为 $a^3=b^3=e$ 和 $ab=b^2a$，又设 G'是由元素 x,y 生成的群，其中 x,y 的定义关系为 $x^2=y^2=(yx)^3=e$，证明 G 与 G'同构.

3. 设群 G 是 24 阶群且 $C(G)=1$，试证 $G\cong S_4$.

4. 令 $G=G_1\times G_2\times\cdots\times G_n$，且对 $\forall\ i\neq j$，$|G_i|$ 和 $|G_j|$ 互素，则 G 的任意子群 H 都是它的子群 $H\cap G(i=1,2,\cdots,n)$ 的直积.

5. 设 G 是有限生成的自由 Abel 群，$\mathrm{rank}(A)=r$，如果 $g_1,g_2,\cdots,g_n$ 是 G 的一组生成元，则 $n\geqslant r$.

6. 设 $H\leqslant G$，且 $[G:H]=n$，证明存在 $K\lhd G$，使得 $K\subseteq H$ 且 $[G:K]\mid n!$.

7. 设 G 是有限群，且 $|G|=2^t m$，其中 $t>0$ 且 m 为奇数. 如果 G 中存在 2^t 阶循环子群，证明 G 中存在子群 K，使得 $[G:K]=2$.

§2.12　群对称性的应用

群论在数字通信、近代物理及计数问题等方面有广泛的应用，下面仅就在计数方面的应用介绍几个问题.

首先解决如何计算集合在群作用下的轨道数目问题.

Burnside 定理　设有限群 G 作用于有限集 S 上，则 S 在 G 作用下的轨道数目为 $N=\frac{1}{|G|}\sum M(g)$，其中 $M(g)$ 为元素 g 在 S 上的不动点数，和式是对每一个群元素求和.

1. 项链问题

设有 n 种颜色的珠子，要做成有 m 颗珠子的项链，问可做成多少种不同种类的项链？

这里所说的不同种类的项链，指两个项链无论怎样旋转与翻转都不能重合. 在数学上可以描述为：

设 $S=\{1,2,\cdots,m\}$，代表 m 颗珠子的集合，它们顺序排列组成一个项链，由于每颗珠子标有号码，我们称这样的项链为有标号的项链. $A=\{a_1,a_2,\cdots,a_n\}$ 为 n 种颜色的集合，则每一个映射 $f:S\rightarrow A$ 代表一个有标号的项链. 令

$$\Pi=\{f\mid f:S\rightarrow A\}=A^S$$

它是全部有标号项链的集合，显然有 $|\Pi|=|A|^{|S|}=n^m$，是全部有标号项链的数目.

现在考虑二面体群 D_m 对集合 Π 的作用. 设

$$g=\begin{pmatrix}1 & \cdots & k & \cdots & m\\ i_1 & \cdots & i_k & \cdots & i_m\end{pmatrix}\in D_m,\quad f=\begin{pmatrix}1 & \cdots & k & \cdots & m\\ c_1 & \cdots & c_k & \cdots & c_m\end{pmatrix}\in\Pi$$

其中 $c_i\in A$. 定义 g 对 f 的作用为

$$g(f)=\begin{pmatrix}g(1) & g(2) & \cdots & g(m)\\ c_1 & c_2 & \cdots & c_m\end{pmatrix}=\begin{pmatrix}i_1 & i_2 & \cdots & i_m\\ c_1 & c_2 & \cdots & c_m\end{pmatrix}=fg^{-1}.$$

则　$e(f)=f, g_1g_2(f)=f(g_1g_2)^{-1}=fg_2^{-1}g_1^{-1}, g_1(g_2(f))=g_1(fg_2^{-1})=fg_2^{-1}g_1^{-1}$，

所以　$g_1g_2(f)=g_1(g_2(f))$.

其意义是，$g\in D_m$ 对 f 的作用就是对项链的点号作一个旋转变换或翻转变换，因而有 $g\in D_m$ 使 $g(f_1)=f_2 \Leftrightarrow f_1$ 与 f_2 是同一类型的 $\Leftrightarrow f_1$ 与 f_2 属于同一轨道.

因此，每一类型的项链对应一个轨道，不同类型项链数目就是 Π 在 D_m 作用下的轨道数目，可用 Burnside 定理求解.

下一个关键问题是：对 $\forall\ g\in D_m$ 如何求 g 在 Π 上的不动点数 $M(g)$，这与 g 的置换类型有关，设 g 是一个 $1^r, 2^s\cdots m^t$ 型置换，g 的轮换分解式可表示为：

$$g=(\cdot)\cdots(\cdot)(\cdot\quad\cdot)\cdots(\cdot\quad\cdot)\cdots,$$

其中有 r 个$(\cdot)$，有 s 个$(\cdot\quad\cdot)\cdots$. 可以证明 $g(f)=f$ 当且仅当上式中同一轮换中的珠子有相同的颜色.

现在来计算 $M(g)=|\{f\,|\,f\in\Pi, g(f)=f\}|$，

而满足 $g(f)=f$ 的 f，对应于 g 的同一轮换中珠子的颜色必须相同，因而每一轮换中的珠子颜色共有 n 种选择. 而 g 所含的轮换个数为 $r+s+\cdots+t$，所以满足条件 $g(f)=f$ 的项链颜色有 $n^{r+s+\cdots+t}$ 种选择，故 $M(g)=n^{r+s+\cdots+t}$，将它代入 Burnside 公式，就得到项链的种类数为：

$$N=1/|D_m|\sum n^{r+s+\cdots+t}(g\text{ 为 }1^r, 2^s\cdots m^t\text{ 型})$$

其中和式是对 D_m 中每一个置换求和. 上式可以进一步表示为：

$$N=1/|D_m|\sum c(r+s+\cdots+t)n^{r+s+\cdots+t}$$

其中 $c(r+s+\cdots+t)$ 为同一类型的群的元素个数，和式是对所有可能的不同置换类型求和.

例 2.12.1　用 3 种颜色做成有 6 颗珠子的项链，可做多少种？

解　由上分析，按类型计算每一个群元素的不动点数，$m=6, D_6\ |\Pi|=3^6$.

1^6 型置换有 1 个，每一个元素的不动点数为 $M(g)=3^6$；

$1^2 2^2$ 型置换有 3 个，每一个元素的不动点数为 $M(g)=3^4$；

2^3 型置换有 4 个，每一个元素的不动点数为 $M(g)=3^2$；

6^1 型置换有 2 个，每一个元素的不动点数为 $M(g)=3$.

所以，$N=1/12\ (3^6+3\times3^4+4\times3^3+2\times3^2+2\times3)=92$.

也可以直接代入公式：$N=1/|D_m|\sum c(r+s+\cdots+t)n^{r+s+\cdots+t}$ 求得.

例 2.12.2　用 3 颗红珠 6 颗白珠做成一个项链，可以做成多少种不同的项链？

解　这个问题与项链问题的一般提法稍有不同，但可用同样的方法来分析. 设 Y 是所有带标号的由 3 颗红珠和 6 颗白珠做成的项链的集合，不难计算出 $|Y|=C_9^3=84$.

群 D_9 作用于集合 Y 上，不同的轨道数目就是所要求的项链的种类数.

为计算 D_9 中每一个元素在集合 Y 中的不动点数，可列表 2.4.

表 2.4

群元素类型	同一类群元素个数	$M(g)$	$\sum M(g)$
1^9 型	1	84	84
$1^1 2^4$ 型	9	4	36
3^3 型	2	3	6
9^1 型	6	0	0
$\sum$	18	126	

所以 $N=126/18=7$. 这 7 种不同的项链如图 2.4 所示.

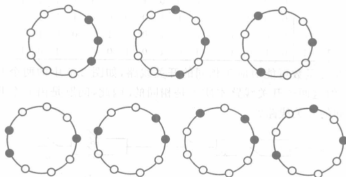


图 2.4

在上面的计算过程中，关键是计算每一个群元素的不动点数，例如对于 3^3 型元素，它的不动点共有 3 个，如图 2.5 所示。

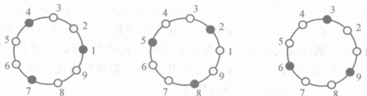


图 2.5

2. 开关线路的计数问题

一个具有两种状态的电子元件称为一个开关，它可由普通的一个开关或联动开关组成. 每个开关的状态由一个开关变量来表示. 由若干个开关 $A_1, A_2, \cdots, A_k$ 组成的一

个线路称为开关线路，一个开关线路也有两个状态，接通用 1 表示，断开用 0 表示，它的状态由各个开关 $A(i=1,2,\cdots,k)$ 的状态决定，因而可用一个函数 $f(A_1,A_2,\cdots,A_k)$ 来表示，f 的取值是 0 或 1，称 f 为开关函数，每个开关线路对应一个开关函数.

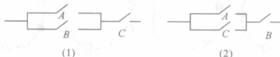
设 $S=\{0,1\}$，则开关函数 $f(A_1,A_2,\cdots,A_k)$ 是 $S\times S\times\cdots\times S$ 到 S 的一个映射. k 个开关变量的开关函数共有 2 的 2^k 次幂个.

例如，当 $k=2$ 时共有 16 个开关函数，列于表 2.5 中：

表 2.5

A	B	$f(A,B)$															
		f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

但不同的开关函数可能对应于相同的开关线路，如图 2.6 中的两个开关线路对应两个开关函数，但这两个开关线路本质上是相同的. 因此，问题是由 n 个开关可组成多少种本质上不同的开关线路？



(1)　　(2)

图 2.6

设 $X=\{A_1,A_2,\cdots,A_n\}$，$G=S_n$ 是 X 上的 n 次对称群. 令 $\Pi=\{f_1,f_2,\cdots,f_m\}$ 是 X 上的所有开关函数的集合(其中 m 等于 2 的 2^n 次幂).

定义 $\sigma\in G$ 对 $f\in\Pi$ 的作用为 $\sigma(f)=f\sigma$，对任何 $A_i\in X$ 有 $\sigma(f)(A_i)=f(\sigma(A_i))$，则由 $\sigma(f_1)=\sigma(f_2)$ 可得 $f_1=f_2$，故 G 是作用于 Π 上的置换群. f_1 和 f_2 对应于本质上相同的开关线路的充要条件是它们在 G 的作用下在同一轨道上，因而本质上不同的开关线路的数目等于 Π 在 G 作用下的轨道数. 可用 Burnside 定理解决此问题.

例 2.12.3　求 $k=3$ 的开关线路的数目.

解　$G=S_3$. 首先，我们来看如何计算 G 中元素 g 的不动点数 $M(g)$.

例如，要求 $g_1=(12)$ 的不动点数 $M(g_1)$，即满足 $g_1(f)=f$ 的开关函数数目，这时要对 f 附加以下条件：$f(0,1,A_3)=f(1,0,A_3)$ 有 6 个函数值 $f(0,0,0)$，$f(0,0,1)$，$f(0,1,0)$，$f(0,1,1)$，$f(1,1,0)$，$f(1,1,1)$ 可任意取值，因而共有 2^6 个函数在 g_1 的作用下不动，所以 $X(g_1)=2^6$.

类似地可求得其他元素的不动点数，列表计算如表 2.6 所示.

表 2.6 S_3 作用在 Π 上的不动点数

群元素类型	$X(g)$	此类群元素个数	每类群元素不动点数之和
1^3 型	256	1	256
$1^1 2^1$ 型	2^6	3	192
3^1 型	2^4	2	32
		$\lvert G\rvert = 6$	$\sum X(g) = 480$

所以 $N = 1/|G| \sum X(g) = 480/6 = 80$，即共有 80 种开关线路.

3. 图的计数问题

首先给出两个图同构的概念：

设 $G_1=(V_1,E_1)$，$G_2=(V_2,E_2)$为两个图，若存在双射

$$\sigma: V_1 \to V_2 \text{ 满足 } (v_i,v_j)\in E_1 \Leftrightarrow (\sigma(v_i),\sigma(v_j))\in E_2,$$

则称 G_1 与 G_2 同构.

直观上看，两个同构的图除点号有区别外是相同的. 下面讨论如何计算不同构的图的数目. 为此，我们要进一步描述此问题.

设 $V=\{1,2,\cdots,n\}$为 n 个点的集合，$Y=\{\{i,j\}\mid i,j\in V, i\neq j\}$是 V 的二元子集的集合，$A=\{0,1\}$，则每一个映射

$$g: Y\to A,$$

对应一个图 $G=(V,E)$，其中 $E=\{\{v_i,v_j\}\in Y \mid g(\{v_i,v_j\})=1\}$

全部 Y 到 A 的映射的集合 $\Pi=\{g\mid g: Y\to A\}=A^Y$.

我们用 Π 同时表示 n 个点上的全部图的集合，则

$$|\Pi|=|A|^{|Y|}=2^t (t=C_n^2)$$

Π 中的图的点都是有标号的.

考虑不同构的图的数目. 定义 n 次对称群 S_n 对 Π 的作用为：

$$\forall \sigma\in S_n, \forall G=(V,E)\in\Pi, \sigma \text{ 对 } G \text{ 的作用为 } \sigma(G)=(V,\sigma(E)),$$

其中 $\sigma(E)=\{\{\sigma(i),\sigma(j)\}\mid\{i,j\}\in E\}$，显然 $\sigma(G)$与 G 是同构的，它们在同一轨道上，因而不同构的图的数目，就是 S_n 作用于 Π 上的轨道数，可用 Burnside 定理求得. 下面的关键问题是求每一个元素 $\sigma\in S_n$ 在 Π 上的不动点数，我们用一个具体问题来说明计算方法.

例 2.12.4 求 4 个点的不同构的图的个数.

解 设 $\Pi=\{(V,E)\mid |V|=4\}$，考虑 S_n 对 Π 的作用，计算 S_n 中每一个元素的不动点数：对元素 e，$M(e)=|\Pi|=2^6=64$. 对 $1^2 2^1$ 型元素，例如$=\sigma(12)(3)(4)$，若 G 是 σ 的不动点，$\sigma(G)=G$，则 G 所对应的映射 $g: Y\to A$ 应有以下限制：$g(\{1,3\})=g(\{2,3\})$，

$g(\{1,4\})=g(\{2,4\})$，因而 Y 中的元素可自由选择函数值的个数为 4，即为：

$$\{1,2\},\{1,3\},\{1,4\},\{3,4\},$$

所以 $M(\sigma)=2^4$.

对 $1^1 3^1$ 型元素，例如 $\tau=(123)(4)$，若 G 满足 $\tau(G)=G$，则 G 所对应的映射 $g: Y\to A$ 必须满足：$g(\{1,2\})=g(\{2,3\})=-g(\{3,1\})$，$g(\{1,4\})=g(\{2,4\})=g(\{3,4\})$，故 Y 中的元素的像可自由选择的元素个数只有 2 个，所以 $M(\tau)=2^2$.

对 2^2 型元素，例如 $\alpha=(1\ 2)(3\ 4)$，类似的分析可得：$M(\alpha)=2^4$.

对 4^1 型元素，例如 $\beta=(1\ 2\ 3\ 4)$，类似的分析可得：$M(\beta)=2^2$.

由 Burnside 定理得：

$$N=1/24(2^6+6\times 2^4+8\times 2^2+3\times 2^4+6\times 2^2)=2^3/24(2^3+6\times 2+4+3\times 2+3)=11$$

4. 分子结构的计数问题

若在苯环上结合 H 或 CH_3 或 NO_2，可形成多少种不同的化合物？

这个问题可分两种情况来考虑：第一种情况，如果把苯环中各连接键看作是等同的，则分子结构问题就是三种颜色的 6 颗珠子的项链问题.

第二种情况，如果把苯环中的连接键看作不同，单键与双键交替时（见图 2.7），则需另外考虑.

例 2.12.5　设苯环上碳原子之间是由单键与双键交替连接的，在每一个碳原子上结合 H 或 CH_3 或 NO_2，问可形成多少种不同的物质（其中有一种化合物为如图 2.7 所示的 TNT 的分子结构）？

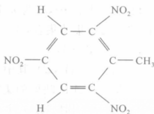


图 2.7

解　这个问题与项链问题的不同之处在于旋转群 G，由于两个分子重合时，必须经过旋转后单键与单键重合，双键与双键重合，故

$G=\{(1),(1\ 3\ 5)(2\ 4\ 6),(1\ 5\ 3)(2\ 6\ 4),(1\ 2)(3\ 6)(4\ 5),(1\ 4)(2\ 3)(5\ 6),(1\ 6)(2\ 5)(3\ 4)\}\cong D_3$.

全部有标号的分子数为 3^6. G 作用于有标号的分子结构上的不动点数计算如表 2.7 所示.

表 2.7

群元素类型	同一类群元素个数	$M(g)$	$\sum M(g)$
1^6型	1	3^6	3^6
3^3 型	2	3^2	2×3^2
2^3 型	3	3^3	3^4
$\sum$	6		$3^2\times 92$

所以 $N=1/6\times 3^2\times 92=138$. 即共可形成 138 种不同的物质,此数比把各键看作等同时要大,因为不对称性增加了.

5. 正多面体着色问题

用 n 种颜色对一个正多面体的顶点着色,用两种着色法经过对正多面体进行着色,如果通过一个旋转能互相重合,则认为这两种着色法本质上是相同的. 问本质上不同的着色法有多少种?

例 2.12.6　用 n 种颜色对正六面体的顶点着色,问有多少种不同的着色方法?

解　我们用类似于项链问题的方法先建立正六面体着色问题的数学模型,设

$X=\{1,2,\cdots,8\}$为正六面体的顶点集合,

$A=\{a_1,a_2,\cdots,a_n\}$为 n 种颜色的集合.

则每一个映射 $f:X\to A$ 对应顶点的一个着色方法,令

$$Y=\{f\mid f:X\to A\}=A^X,$$

为全体着色方法的集合,则得 $|Y|=|A|^{|X|}=n^8$为正六面体顶点的全部着色法数目.

但是在这些着色法中,有些着色法可通过正六面体的一个旋转使它们重合,即这些着色法本质上是相同的. 那么本质上不同的着色法的数目是多少呢?这就涉及正立方体的旋转群 G 对集合 Y 的作用问题.

在立方体的旋转群中,其中 1^8 型置换 1 个,4^2 型置换 6 个,2^4 型置换 9 个,$1^2 3^2$ 型置换 8 个,对每一个类型置换计算不动点数,或直接代入公式即得:

$$N=1/24(n^8+6n^2+9n^4+8n^4)=1/24(n^8+17n^4+6n^2).$$

第3章 群表示论

群表示理论是群论的核心内容之一，是代数表示论的一个重要分支. 它对群论本身以及对物理、化学等其他学科都有着广泛的应用.

有限群的表示理论大致可分为两类：一为常表示论，一为模表示论. 前者在有限群的发展中起了很大作用，后者对于有限单群分类问题的解决提供了有力的工具. 因而本章将有限群的表示与有限结合代数的表示放在一起介绍，侧重介绍有限群的特征标理论及其应用.

关于对称群论的应用，物理或工程系统的许多最重要性质均依赖于系统的对称性，相应的对称性往往可以用不同的对称群描写. 只要能找到与这些对称群同构的一般线性矩阵群（即所谓表示）就可以从矩阵群的结构（矩阵群的结构便于分析）知道相应对称群的结构，从而获得对应系统的许多对称性质和演化规律的认识.

§3.1 结合代数

我们将介绍既有环结构又有向量空间结构的一个代数系统——结合代数，首先介绍代数的有关概念及例子，并介绍一些基本结果.

定义 3.1.1 域 F 上向量空间 A 称为一个 F 上的代数，或 F 代数，简称代数，如果在 A 中规定一个乘法运算满足下列条件：

1）对 $\forall\ a,b,c\in A, a(b+c)=ab+ac, (b+c)a=ba+ca$；

2）对 $\forall\ k\in F, a,b\in A, (ka)b=k(ab)=a(kb)$.

定义 3.1.2 代数 A 称为有限维代数，若它作为 F 向量空间是有限维的. 若 $\dim_F A=n$，则称 A 为 n 次代数.

定义 3.1.3 A 称为交换代数，若代数 A 的乘法适合交换律，即对于 $\forall\ a,b\in A, ab=ba$.

定义 3.1.4 A 称为结合代数，若代数 A 的乘法适合结合律，即对 $\forall\ a,b,c\in A$，$a(bc)=(ab)c$，按照定义，一个结合代数 A 既是 F 上一个向量空间又是一个环，且满足某种“结合律”.

定义 3.1.5　A 称为 Lie 代数，若代数 A 的乘法适合条件：对于 $\forall\ a,b,c\in A, a^2=0, (ab)c+(bc)a+(ca)b=0$.

定义 3.1.6　A 称为 Jordan 代数，若代数 A 的乘法适合条件：对于 $\forall\ a,b,c\in A, ab=ba, (a^2b)a=a^2(ba)$.

定义 3.1.7　A 称为交错代数，若代数 A 的乘法适合条件：对于 $\forall\ a,b\in A, a(ab)=(aa)b, a(bb)=(ab)b$.

从对数学及物理的广泛应用的角度来说，以上几类代数中最重要的而又经常出现的是结合代数. 结合代数的一个最典型的例子是有限维向量空间上所有线性变换作成的代数；从理论上来讲，抓住了这个代数，可以说抓住了"所有"的代数，因为任何一个有限维结合代数都与这个代数的某个子代数同构. 这完全类似于对称群在群论中的地位. 鉴于以上原因及我们的需要，我们侧重学习有限维结合代数.

结合代数与环的差别在于环的加群只是一个交换群，而代数的加群是一个域 F 上的向量空间，于是，代数比环就有一个结构简单得多的加群；下面我们看一看如何确定一个有限维结合代数.

设 A 是一个有限维代数，A 作为向量空间，设 $a_i(i=1,2,\cdots,n)$ 是 A 的一个基，于是 A 中任意元素 a 都可唯一表示为

$$a=\sum_{i=1}^{n}k_ia_i, k_i\in F.\text{若 } b\in A,\text{而 } b=\sum_{i=1}^{n}h_ia_i, h_i\in F,\text{则 } ab=\sum_{i,j}k_ih_ja_ia_j,$$

这说明基元 a_i 之间的乘法表完全确定了整个代数 A 的乘法运算. 易见 A 是结合代数当且仅当基元之间的乘法运算满足结合律. 令

$$a_ia_j=\sum_{r=1}^{n}\delta_{ij}^{(r)}a_r, \delta_{ij}^{(r)}\in F,$$

因为

$$a_i(a_ja_k)=\sum_{s=1}^{n}\delta_{jk}^{(s)}a_ia_s=\sum_{t=1}^{n}\left(\sum_{s=1}^{n}\delta_{jk}^{(s)}\delta_{ij}^{(t)}\right)a_t,$$

$$(a_ia_j)a_k=\sum_{t=1}^{n}\left(\sum_{s=1}^{n}\delta_{ij}^{(s)}\delta_{sk}^{(t)}\right)a_t,$$

于是

$$\sum_{s=1}^{n}\delta_{ij}^{(s)}\delta_{sk}^{(t)}=\sum_{s=1}^{n}\delta_{jk}^{(s)}\delta_{is}^{(t)},$$

其中 $i,j,k,t=1,2,\cdots,n$.

若 F 上向量空间有基 a_i，其中任意元 $a=\sum_{i=1}^{n}k_ia_i$ 与 $b=\sum_{i=1}^{n}h_ia_i$ 的乘积由 $ab=$

$\sum_{i,j} k_i h_j a_i a_j$ 来规定，并且 $\delta_{ij}^{(r)}$ 又适合上式，易证 A 是 F 上代数.

由以上讨论可知，域 F 上有限维代数 A 的构造由 F 中适合上式的 n^3 个元 $\delta_{ij}^{(r)}$ 唯一确定. $\delta_{ij}^{(r)}$ 称为 A 的构造元素. 一个已知域的代数如何确定，是代数的主要问题之一，对某些特殊类型的代数，这个问题已完全解决.

定义 3.1.8 一个代数 D 称为可除代数，如果 D 的非零元对乘法构成一个群，按照定义，域 F 的扩张是 F 上一个可除代数. 实数域、复数域和四元数除环分别是实数域上的 1 次、2 次及 4 次可除代数.

有趣的是，这三个代数就是实数域上所有可能的有限可除代数. 这就是下面著名的 Frobenius 定理.

定理 3.1.1 D 是实数域上的可除代数$\Leftrightarrow D$ 是实数域、复数域和四元数除环.

证明 设 $\mathbf{R}$ 是实数域，D 是 $\mathbf{R}$ 上的 n 次可除代数.

若 $n=1$，则 $D=\mathbf{R}$，即 D 是实数域.

若 $n>1$，则 D 中有不为实数的数 α，α 是 $\mathbf{R}$ 上的代数元. 因为 $\mathbf{R}[x]$ 中不可约多项式的次数是 1 或 2，而 $\alpha \notin \mathbf{R}$，故在 $\mathbf{R}[x]$ 中 α 适合的不可约多项式的次数是 2. 假设这个不可约多项式是 x^2+px+q，因为它没有实根，故判别式 $p^2-4q<0$，设 $q-p^2/4=h^2$，其中 h 为实数，于是 D 中元 $i=(\alpha+p/2)/h$ 满足 $i^2=-1$，即 i 满足不可约多项式 $x^2+1=0$，于是 $\mathbf{R}(i)$ 是 $\mathbf{R}$ 的 2 次扩域.

若 $n=2$，则 $D=\mathbf{R}(i)$，因为 $\mathbf{R}(i)$ 与复数域 $\mathbf{C}$ 同构，故 D 是复数域.

若 $n>2$，首先我们证明四元数除环包含在 D 中. 因为 $n>2$，同上面一样，D 含有 $\mathbf{R}(i)$ 外的元素 j_0，于是 $j_0^2=-1$.

下面计算 ij_0 及 $j_0 i$，因为 D 中任意元是 $\mathbf{R}[x]$ 中 2 次多项式的零点，当然 $i+j_0$，$i-j_0$ 也是. 于是我们有

$$(i+j_0)^2=-2+ij_0+j_0 i=a(i+j_0)+b(i-j_0)^2=-2-ij_0-j_0 i=c(i-j_0)+d$$

其中 $a,b,c,d\in\mathbf{R}$，将上面两式相加得

$$-4=(a+c)i+(a-c)j_0+(b+d)$$

因为 $j_0\notin\mathbf{R}(i)$，故 $1,i,j_0$ 在 $\mathbf{R}$ 上线性无关，因此 $a+c=0$，$a-c=0$，也即 $a=0$，$c=0$. 故 $ij_0+j_0 i=2t$，$t=(b+2)/2$.

我们求四元数除环中的 j，令 $j'=j_0+ti$，则

$$ij'+j'i=i(j_0+ti)+(j_0+ti)i=ij_0+j_0 i-2t=0,$$

$$(j')^2=-1+t(ij_0+j_0 i)-t^2=-1+t^2$$

必为负数，即 $(j')^2<0$. 否则若 j' 是实数，则 $1,i,j_0$ 就线性相关，与假设矛盾.

令 $j(j')^2=-s^2$，$s\in\mathbf{R}$，则 $j=(1/s)j'$，

于是 $j^2=-1$，且 $ij+ji=((1/s)^2s)(ij'+j'i)=0$，

亦即 $ij=-ji$. 设 $k=ij$，得 $ij=-ji=k$. 再由计算易得

$$k^2=-1, ki=-ik=j, jk=-kj=i$$

设 $k=a+bi+cj, b, a, b, c\in\mathbf{R}$，用 i 左乘该式的两边得

$$-j=ai-b+ck=ai-b+c(a+bi+cj)=ca-b(a+bc)i+c^2j$$

因为 $1, i, j$ 线性无关，故 $c^2=-1$，这与 c 为实数的假设矛盾. 由此得 $1, i, j, k$ 线性无关. 这就说明 D 含有所有四元数 $a+bi+cj+dk$，从而 D 含有四元数除环. 若 $n+4$，则 D 是四元数除环.

最后我们证明 $n\leqslant 4$. 设 $n>4$，则 D 中又有元素 $l^2=-1$，且它与 $1, i, j, k$ 线性无关. 我们有

$$il+li=a, jl+lj=b, kl+lk=c, a, b, c\in\mathbf{R}.$$

于是

$$lk=(li)j=aj-ilj=aj-i(b-jl)=aj-bi+ijk=aj-bi+ki=aj-bi+c-lk$$

因此 $aj-bi+c=2ik$. 用 k 右乘该式两边得 $a+bi+cj=-2l$.

这与 i, j, k, l 线性无关的假设矛盾，故 $n\leqslant 4$. 结论得证.

下面我们介绍代数的有关概念，对于 F 代数来说也有诸如子代数、(左、右、双边)理想、商代数、代数的同态、直和等概念及有关的同态基本定理.

定义 3.1.9 设 B 是域 F 上代数 A 的一个非空子集合，B 称为 A 的子代数，若 B 是 A 的子空间 A 又是 A 的子环.

定义 3.1.10 B 称为 A 的左(右)理想，若 B 是 A 的子代数且又是 A 的左(右)理想.

B 称为 A 的理想，若 B 既是 A 的左理想又是 B 的右理想.

定义 3.1.11 若 B 是 A 的理想，则 $A/B=\{a+B\mid a\in A\}$，既是一个环又是一个商空间，称 A 关于理想 B 的商代数.

需要注意的是，因为代数有单位元 1，我们有 $F\cdot 1=\{f\cdot 1\mid f\in F\}$ 是 A 的子代数，A 的中心

$$Z(A)=\{a\in A\mid ax=xa, \forall\ x\in A\}$$

也是 A 的子代数，且 $F\cdot 1\subseteq Z(A)$. 若 A 无单位元，则 F 不一定包含在 A 中.

定义 3.1.12 设 A 和 B 都是域 F 上的代数，f 是集合 A 到 B 的一个映射，f 称为代数 A 到代数 B 的一个同态映射.

若 f 既是环 A 到环 B 的一个同态映射，又是向量空间 A 到向量空间 B 的一个线性映射. 换句话说，对$\forall\ a, b\in A, k\in F$ 都有

$$f(a+b)=f(a)+f(b), f(ab)=f(a)f(b), f(ka)=kf(a).$$

此时我们说代数 A 和代数 B 同态，记为 $A\sim B$，

$\mathrm{Ker}f=\{x\in A\mid f(x)=0\}$ 称为 f 的同态核.

若 f 既是满射又是单射，称代数 A 和代数 B 同构，记为 $A\cong B$.

前面我们看到，利用代数的构造元素可以构造一些有限维结合代数.

另一方面，与群的内、外直和概念相类似，利用已知的一些代数通过一定的方法可构造出新的代数. 也可以把一个代数分解成一些子代数的和.

定义 3.1.13　设 $A_i(i=1,2,\cdots,n)$ 是 F 上的有限维代数，令

$$A=\{(a_1,\cdots,a_n)\mid a_i\in A_i,1\leqslant i\leqslant n\}$$

规定 $\{a_1,\cdots,a_n\}=\{b_1,\cdots,b_n\}$ 当且仅当 $a_i=b_i,1\leqslant i\leqslant n$. 定义其运算为

$$k\{a_1,\cdots,a_n\}=\{ka_1,\cdots,ka_n\}$$

$$\{a_1,\cdots,a_n\}+\{b_1,\cdots,b_n\}=\{a_1+b_1,\cdots,a_n+b_n\}$$

$$\{a_1,\cdots,a_n\}\{b_1,\cdots,b_n\}=\{a_1b_1,\cdots,a_nb_n\}$$

则可验证 A 为 F 上有限维代数.

其中 $\dim_F A=\sum_{i=1}^{n}\dim_F A_i$，称代数 A 为代数 $A_1,\cdots,A_n$ 的外直和.

定义 3.1.14　设 A 是一个有限维代数，$A_1,\cdots,A_n$ 是 A 的子代数，若每个 $A_i(1\leqslant i\leqslant n)$ 是代数 A 的理想，且 A 作为向量空间是 $A_i(1\leqslant i\leqslant n)$ 的直和，则称代数 A 是其子代数 $A_i(1\leqslant i\leqslant n)$ 的内直和.

无论 A 是哪种直和，都把 A 记为

$$\Sigma_i\oplus A_i=A_1\oplus\cdots\oplus A_n.$$

定义 3.1.15　对于一个代数 B，我们可定义一个新的代数 B^{op}，它的元素以及它的加法运算和数乘运算与 B 相同，它的乘法运算是 B 的反运算，即 $\forall\ a,b\in B$，若用 ab 表示 B 的乘法运算，$a\cdot b$ 表示 B^{op} 的乘法运算，规定 $a\cdot b=ba$. 容易验证，B^{op} 关于上述运算作成一个代数，称为代数 B 的反代数. 关于反代数，下列事实是明显的：

1) $(B^{op})^{op}\cong B$；

2) 若 B 是可除代数，则 B^{op} 也是可除代数.

3) 若 B 是若干个代数的直和，则 B^{op} 也是若干个反代数的直和.

定义 3.1.16　一个代数 A 称为单代数，如果它的理想只有零理想和它自身. 显然，可除代数一定是单代数.

反之不然. 下面我们给出一个极其重要的单代数的例子.

例 3.1.1　设 A 是一个有单位元的环，M 是一个 A 模，则 $\mathrm{End}_A(M)$ 的乘法运算是映射的合成，它的加法运算和数乘运算按通常的定义，关于这些运算，$\mathrm{End}_A(M)$ 是一个 F 代数称为 M 的自同态代数. 特别地，若 F 是域，M 是 F 上的 n 维向量空间，则 End_F

$(M)\cong M_nL(F)$,后者的运算为矩阵的加法、乘法和数乘,其维数为 n^2,这是一个单代数,由此可见,单代数不一定是可除代数.

另外两个重要的结合代数的例子是零乘代数与幂零代数.

定义 3.1.17 设 A 为域 F 上的 n 维向量空间,规定 A 中任意两个元素的乘积都是零,A 是一个结合代数,称为零乘代数.

若一个代数 A 满足 $A^n=0$,则称 A 为幂零代数.

设 $1<n$ 为正整数,N 为域 F 上所有的主对角线元素均为零的 $n\times n$ 上三角矩阵作成的集合,则 N 关于矩阵的加法、乘法和数乘作成 F 上的代数.可以验证

$$\dim_F N=1+2+\cdots+(n-1)=n(n-1)/2,$$

且 N 中任意 n 个元素之积必为零,或 $N^n=0$,于是 N 是幂零代数.

上面我们给出了一些代数的例子,在这些例子中,可除代数和零乘代数是两极端类型,单代数接近可除代数而较之宽,幂零代数靠近零乘代数而较之广.研究单代数与幂零代数这两类有鲜明特点的代数类,并利用它们去刻画任意有限维结合代数,是今后讨论结合代数结构的主要途径之一.

Gauss 小传

高斯(C. P. Gauss),德国数学家、物理学家和天文学家,1777 年 4 月 30 日生于不伦瑞克,1855 年 2 月 23 日卒于格丁根.Gauss 是近代数学的奠基者之一,在历史上影响之大,可以和阿基米德、牛顿、欧拉并列.Gauss 出生在一个贫苦的家庭里,父亲本不打算让他上学,但他很小就显示出有数学才能,十岁时就开始学习代数和分析.1795 年由于好友的推荐,得到一个公爵的资助,进入格丁根大学学习,他的一生就在格丁根度过.19 岁时,Gauss 发现了正十七边形的尺规作图法,这是欧几里得以来悬而未决的问题.

1799 年,Gauss 在普法夫(J. F. Phs)的指导下获得博士学位,在他的学位论文中,他证明了代数基本定理.1801 年,Gauss 出版了他数论方面的不朽巨著《算术探究》,该书系统总结了以前的工作,并引入了许多他自己的一些基础性的思想,包括模算术的概念.此书奠定了近代数论的基础.1801 年,Gauss 经过几个星期的努力,创立了行星椭圆轨道法,利用有限的几个观测数据计算出了一颗当时未知行星的轨道,以后天文学家在预测的位置上重新找到了这颗星(谷神星).Gauss 后来总结了这种方法,写成《天体沿圆锥曲线绕日运动的理论》,在书中他还首次阐述了最小二乘法原理.

1807 年,Gauss 成为天文学教授,并担任了格丁根大学新天文台的台长.在以后的几十年中,Gauss 不仅继续在数学的几乎所有分支中作出重要贡献,而且在天文学、力学、电磁学、光学、测地学等领域也有很大贡献.他与别人共同发明了电磁电报.现在磁通量密度的单位就是以高斯命名的.由于 Gauss 对复数的使用,才使得许多数学家接

受了复数.复数的名称也是由 Gauss 推广开的.他还推广了用 i 来表示 $\sqrt{-1}$.他证明了 $\mathbf{Z}_{[i]}$是唯一分解整环.Gauss 还培养了许多著名的数学家,如黎曼(Riemann)、库默尔、戴德金、艾森斯坦因(Eisenstein)等.

问题 3.1

1.证明:关于代数的同态基本定理,第一、二同构定理.

2.设 $A_1,\cdots,A_n$ 是域 F 上代数 A 的理想,求证下列条件是等价的:

(1)$A=\sum_{i=1}^{n}\oplus A_i$;

(2)作为 F 上的向量空间,$A=\sum_{i=1}^{n}A_i$,且 $\dim_F A=\sum_{i=1}^{n}\dim_F A_i$;

(3)A 中元素可唯一表成 A_i 中元素的和;

(4)存在向量空间 A 到 A_i 上的同态映射 φ_i 满足 $\varphi_i\varphi_j=a_{ij}\varphi_i$,且 $\Sigma_i\varphi_i=1$,其中 1 是 A 的恒等自同构.

3.代数 A 的子代数 B 称为 A 的直和因子,若存在 A 的子代数 B' 使得 $A=B\oplus B'$,证明:若 B 是 A 的直和因子,则 B 的理想 B_1 也是 A 的理想.

4.设 A 是域 F 上代数,对于 $a\in A$,令 $R_a: x\longmapsto xa, x\in A$.证明:

(1)R_a 是向量空间 A 的一个线性变换;

(2)令 $A_R=\{R_a|a\in A\}\subseteq \mathrm{End}_F(A)$,则 A_R 关于线性变换的运算是 F 代数;

(3)$\varphi: a\longmapsto R_a, a\in A$,是代数 A 到代数 A_R 的同构映射,因而任何一个代数可看作 A 的自同态代数的子代数.

§3.2　有限维代数

这一节我们讨论在有限群表示论中占有极其重要地位的另一个有限维代数的例子——群代数.

定义 3.2.1　设 G 为群,F 是域,令 $FG=\{\Sigma_{g\in G}k_g g\,|\,k_g\in F\}$.规定

$$\Sigma_{x\in G}k_x x+\Sigma_{x\in G}h_x x=\Sigma_{x\in G}(k_x+h_x)x$$

$$(\Sigma_{x\in G}k_x x)(\Sigma_{x\in G}h_x x)=\Sigma_{x\in G}\Sigma_{y\in G}k_x h_y xy$$

$$=\Sigma_{x\in G}(\Sigma_{y\in G}k_y h_{y^{-1}x})x,$$

$$\lambda(\Sigma_{x\in G}k_x x)=\Sigma_{x\in G}(\lambda k_x)x, \lambda\in F.$$

则 FG 按上述运算作成一个代数,称为 F 上的群代数.

F 的单位元 1 就是 FG 的单位元.G 中元素是 FG 的一个基,因而若 G 为有限群,

则 FG 是有限维的且 $\dim(FG)=|G|$.

若把群代数 FG 看作一个环，则 FG 模 M 也可看作为一个 F 向量空间.

事实上，对 $\lambda\in F, m\in M$，令 $\lambda m=(\lambda 1)m$，则 M 关于这个运算以及它的加法运算就构成向量空间. 当 G 为有限群时，我们有下列关系.

引理 3.2.1　设 F 是域，G 是有限群，则 FG 模 V 是有限生成的当且仅当 V 作为 F 向量空间是有限维的.

证明　设 V 作为 FG 模是有限生成的，其中 V 的生成元集为 $\{v_1,\cdots,v_t\}$，向量空间可由 $\{gv_i \mid g\in G, 1\leqslant i\leqslant t\}$ 生成，因为 G 有限，由此 $\dim V<\infty$.

反之是显然的.

下面我们给出群代数上的模与线性表示之间的一个基本联系.

我们学习了群在集合上的作用，现在介绍群在向量空间上的作用.

定义 3.2.2　设 F 是一个域，G 是一个群，令 G 作用在一个向量空间 V_F 上，我们说 G 在 V_F 上的作用是线性的，如果下列条件成立：

1) 对$\forall\ g\in G, v, u\in V$ 都有 $g(u+v)=gv+gu$；

2) 对$\forall\ g\in G, a\in F, v\in V$ 都有 $g(av)=a(gv)$；

由第二章知群 G 在集合 X 上的一个作用对应于群 G 到对称群 Σ_x 内的一个同态，对于群 G 在向量空间 V_F 上的线性变换而言，我们有下列结果

定理 3.2.2　群 G 在向量空间 V_F 上的线性变换组成的集合与群 G 到 $GL(V)$ 上的同态组成的集合之间有一个一一对应.

证明　设 $f: G\to GL(V)$ 是一个同态，定义 $gv=f(g)(v)$，则容易验证这是 G 在 V_F 上的一个线性变换.

反之，若给定 G 在 V 上的一个线性变换，则我们可定义一个同态：

$$f: G\to GL(V),$$

其中 $f(g)(v)=gv, g\in G, v\in V$.

可以验证上述过程是互逆的，这样就完成了证明.

上命题中的同态

$$f: G\to GL(V)$$

称为 G 在 V 中的一个线性表示. 由上命题可知，群的线性表示的研究等价于群的线性变换的研究，这里的群一般侧重于有限群，向量空间一般侧重于有限维向量空间. 群的线性表示这个研究领域起源于 19 世纪后期，并且已经证明对有限群的研究有许多应用.

引理 3.2.3　设 F 是域，G 是有限群，则在所有有限生成 FG 模组成的集合与 G 在有限维向量空间上的线性变换组成的集合之间有一个一一对应.

证明　若 V 是有限生成 FG 模，则 $\dim_F V<\infty$. 限制模映射 $FG\times V\to V$ 到 $G\times V$ 上，就得到 G 在 V 上的一个线性变换. 反之，设 V 是有限维 F 向量空间，G 线性作用在 V 上，则对于 $v\in V$，$a_g\in F$，$\Sigma_{g\in G}a_g g\in FG$，令

$$(\Sigma_{g\in G}a_g g)v=\Sigma_{g\in G}a_g(gv).$$

容易验证，FG 作用在 V 上(这个作用也称为 G 在 V 上的作用的线性扩张)，因而 V 是一个 FG 模. 可以验证这些过程是互逆的，结论得证.

由上述可得，为了在向量空间 V_F 上定义一个 FG 模，只要规定一个 G 在 V 上的作用即可. 而 FG 在 V 上的作用定义为 G 在 V 上的作用的线性扩张.

以下设 F 是域，G 是有限群，所有的向量空间 V_F 都是有限维的，所有的 FG 模都是有限生成的.

定义 3.2.3　对于 $g\in G$，$a\in F$，令 $ga=a$，则 F 可看作 FG 模. F 称为平凡 FG 模，简称为平凡模.

定义 3.2.4　设 G 作用在有限集 X 上，FX 表示 X 中元的所有 F 线性组合作成的集合，则 FX 是一个 F 向量空间，其基为 X. 设 $X=\{x_1,\cdots,x_n\}$，对于 $g\in G$，$\Sigma_i c_i x_i\in FX$，我们有 $g(\Sigma_i c_i x_i)=\Sigma_i c_i(gx_i)$. 把这个作用线性扩张到 FG，则 FX 是一个 FG 模. FX 称为置换 FG 模，简称为置换模.

设 U 和 V 是 FG 模，对于 $g\in G$，令 $g(u,v)=(gu,gv)$，则 $U\oplus V$ 是 FG 模. 另外我们已知 $U\odot_F V$ 和 $\mathrm{Hom}_F(U,V)$ 是 F 向量空间.

下面我们将说明这两个模也可以作成 FG 模.

对于 $g\in G$，令 $g(u\odot v)=gu\odot gv$，把这个作用线性扩张到 FG，则 $U\odot_F V$ 是一个 FG 模. 对于 $g\in G$，$u\in U$，$f\in \mathrm{Hom}r(U,V)$，令 $(gf)(u)=g(f(g^{-1}u))$，则容易验证 $gf\in \mathrm{Hom}r(U,V)$.

又对于 $g_1,g_2\in G$，我们有

$$\begin{aligned}((g_1g_2)f)(u)&=g_1g_2f(g_1g_2)^{-1}u)=g_1(g_2f(g_2^1(g_1^{-1}(u)))\\&=g_1((g_2f)(g_{-1}^{-1}u))=(g_1(g_2f))(u)\end{aligned}$$

这说明 $(g_1g_2)f=g_1(g_2f)$，由此易得 $\mathrm{Hom}r(U,V)$ 是一个 FG 模. 令 $U^*=\mathrm{Hom}r(U,F)$，其中 F 看作平凡模. U^* 称为 U 的对偶模，这里 $gf(u)=f(g^{-1}u)$.

可以证明，$U^*\odot_F V$ 与 $\mathrm{Hom}_F(U,V)$ 是同构的 FG 模.

下面我们证明有限群表示理论中的一个最基本结果，它是由 H. Maschke 于 1898 年发现的.

Maschke 定理　设 G 是群，$\mathrm{char}F=0$ 或 $\mathrm{char}F$ 不整除 $|G|$，如果 U 是一个 FG 模且 V 是 U 的一个 FG 子模，则作为 FG 模，V 是 U 的一个直和因子.

证明　因为 U，V 是 FG 模，当然 U，V 也是 F 向量空间. 作为 F 向量空间，由线性

代数知道，存在 U 的一个 F 子空间 W 使 $U=V\oplus W$.

令 $\pi: U\to V$ 是 U 在 V 上沿 W 的投影，即若 $u=v+w$，其中 $u\in U, v\in V, w\in W$，则 $\pi(u)=v$，故 π 是使得 $\pi(v)=v, v\in V, \pi(w)=0, w\in W$ 的唯一的线性变换. 对于 $u\in U$，再定义 U 到 U 的线性变换 π' 为

$$\pi'(u)=\frac{1}{|G|}\sum_{g\in G}g\pi(g^{-1}u).$$

因为 V 是 U 的 FG 子模，所以对于 $g\in G, v\in V$，我们有 $gv\in V$. 由此可见 π' 把 U 映射到 V，又因为 π' 在 V 上是恒等的，因而对 $\forall\, g\in G, v\in V$，我们有 $g\pi(g^{-1}v)=gg^{-1}v=v$，因而 π' 在 V 上的限制是恒等的，作为 F 向量空间，由线性代数知 $U=V\oplus \mathrm{Ker}\pi'$.

下面我们只需证明 $\mathrm{Ker}\pi'$ 是 U 的 FG 子模. 为此只需证明 π' 是 FG 模同态，即只需证明对 $\forall\, x\in G, u\in U, \pi'(xu)=x\pi'(u)$. 首先我们有

$$\begin{aligned}\pi'(xu)&=\frac{1}{|G|}\sum_{g\in G}g\pi(g^{-1}xu)=\frac{1}{|G|}\sum_{g\in G}xx^{-1}g\pi(g^{-1}xu)\\&=\frac{1}{|G|}x\Big(\sum_{g\in G}x^{-1}g\pi(g^{-1}xu)\Big)\end{aligned}$$

当 g 取遍 G 中元时，对于固定的 $x\in G, y=x_1g$ 也取遍 G 中元，因而适当替换变量后我们有

$$\pi'(xu)=x\Big(\frac{1}{|G|}\sum_{g\in G}y\pi(y^{-1}xu)\Big)=x\pi'(u).$$

定理 3.2.4 设 F 是域且 $\mathrm{char}F$ 不整除 $|G|$，则每一个非零 FG 模是半单的.

证明 设 U 是非零 FG 模，对 $\dim_F U$ 用归纳法. 若 U 是单模，则结论成立. 这说明 $\dim_F U=1$ 的情况已证.

设 $\dim_F U>1$ 且 U 不是单模，则 U 必有一个非零真子摸 V，由 Maschke 定理，存在 U 的非零真子模 W 使得 $U=V\oplus W$. 又 $\dim_F V, \dim_F W<\dim_F U$，由归纳假设，$V$ 和 W 是半单的，从而 U 是半单的.

Hamilton 小传

哈密尔顿(W. R. Hamilton)是爱尔兰数学家、物理学家，1805 年 8 月 4 日生于爱尔兰的都柏林. Hamilton 五岁时就能读拉丁语、希腊语和希伯来语，14 岁时已学会了 12 种语言. 1823 年进入都柏林三一学院学习. 1827 年，当他才 22 岁还是大学生时，便被任命为邓辛克天文台台长及都柏林三一学院天文学教授，并获皇家天文学家称号. 1832 年成为爱尔兰科学院院士，1837—1845 年任院长.

Hamilton 在数学上的主要成就是发现了四元数和发展了变分法及微分方程的理

论. 四元数是复数的自然推广，四元数中的 i、j、k 的平方都是 -1，利用它们，三维和四维中的旋转可以进行代数化的处理. 但最重要的是，四元数关于乘法运算是不交换的！这是当时发现的第一个不满足交换性的环.

Hamilton 后来回忆道：在经历了 15 年的冥思苦想之后，智慧的火花某一天突然在他的大脑中迸发. 那是 1843 年 10 月 16 日，星期一，当 Hamilton 沿着皇家运河步行去爱尔兰科学院的路上时，他的脑海中闪现出了如下的一串基本公式：

$$i^2=j^2=k^2=ijk=-1.$$

这包含了他 15 年来所考虑的问题的全部解. 他迅速地把这记录在随身携带的笔记本中，并在路过运河边的一座小桥时，用小刀将公式刻在了桥边的石头上.

克莱因(M. Klein)后来评价说：四元数的发现"对代数学具有不可估量的重要性". 以 Hamilton 名字命名的术语有：Hamilton 函数(它代表了物理系统中的总能量). 哈密尔顿—雅可比微分方程以及线性代数中的凯莱—哈密顿定理等. 而向量、标量、张量等术语的使用也归功于 Hamilton.

Hamilton 于 1865 年 9 月 2 日在都柏林附近的邓辛克天文台逝世，享年 60 岁.

问题 3.2

1. 设 U 和 V 是 FG 模，则 $U^*\odot_F V$ 与 $\mathrm{Hom}_F(U,V)$ 是同构的 FG 模.

2. 设 F 是域 G 的有限群，证明：

(1) $a=\Sigma_{g\in G}g\in FG$，则 Fa 是 FG 中与平凡模同构的唯一的子空间；

(2) $f: FG\to F$ 是 FG 模的满同态，其中对于 $g\in G$，$f(g)=1$，则 $\mathrm{Ker}f$ 是 FG 的使得 $FG/\mathrm{Ker}f$ 同构于平凡模的唯一的子模；

(3) 设 $\mathrm{char}F\,|\,|G|$，则 $Fa\subseteq\mathrm{Ker}f$(由此得 $\mathrm{Ker}f$ 不是 FG 的直和因子)，因此 FG 模不是半单模.

§3.3　半单代数的对称性

本节涉及的代数均指有单位元的有限维 F 代数，其中 F 是一个域. 代数上的模均指有限生成模，模的直和也假设是有限的.

定义 3.3.1　代数 A 是半单的，如果所有的非零 A 模是半单的.

如果 G 是有限群且 F 的特征不整除 $|G|$，则群代数 FG 是半单的.

下面我们介绍半单代数的某些基本结果. 首先，我们来决定在什么条件下，一个且模是半单的.

引理 3.3.1　对于一个 A 模 M 来说，下列条件是等价的：

(1)M 的任何子模是 M 的直和因子；

(2)M 是半单模；

(3)M 是一些单子模的和.

证明 (1)⇒(2)，与推论 5.3.4 类似证明.(2)⇒(3)，由定义直接可得.

(3)⇒(1)，假设(3)成立，N 是 M 的一个子模. 令 $V=\max\{W\subset M\mid W\cap N=0\}$，其中 W 是 M 的子模. 我们希望证明 $N+V=M$.

设 $N+V\subset M$，如果 M 的每一个子模均含在 $N+V$ 中，由(3)知，$M\subseteq N+V$，矛盾. 因而必有 M 的一个单子模 S 不含在 $N+V$ 中，因为 $S\cap(N+V)$ 是单子模 S 的真子模，故 $S\cap(N+V)=0$，当然 $S\cap V=0$，于是我们有 $V\subset V+S$. 令 $n\in N\cap(V+S)$，则存在 $v\in V$，$s\in S$ 使得 $n=v+s$. 由此得 $s=n-v\in S\cap(N+V)$，因而 $s=0$，也即 $n=v$，因为 $N\cap V=0$，所以 $n=0$. 由此得 $N\cap(V+S)=0$. 这与 V 的极大性假设矛盾，因而我们有 $M=N+V$. 又因为 $N\cap V=0$，故 M 是 N 与 V 的直和，即 N 是 M 的直和因子，这就得出(1)成立.

引理 3.3.2 半单模的子模和商模也是半单模.

证明 设 M 是一个半单 A 模，由引理 3.3.1 可知，M 的每一子模都同构于 M 的某个商模，于是只要证明 M 的每个商模是半单模即可. 令 M/N 是一个商模，$f: M\to M/N$ 是一个自然模同态，因为 M 是半单的，则 M 是一些单子模的直和. 不妨设 $M=S_1+S_2+\cdots+S_n$，于是 $M/N=f(M)=f(S_1)+f(S_2)+\cdots+f(S_n)$. 由模同态基本定理，$f(S_i)$ 同构于 S_i 的某一个商模，但 S_i 是单模，故 $f(S_i)=0$ 或 $f(S_i)$ 是单模，因而 M/N 是单子模的和. 由引理 3.3.1 知，M/N 是半单模.

引理 3.3.3 代数 A 是半单的当且仅当 A 模 A 是半单的.

证明 设 A 模 A 是半单的，M 是由 $\{m_1,\cdots,m_r\}$ 生成的 A 模. 令 A^r 表示 r 个 A 模 A 的直和，定义

$$f:(a_1,\cdots,a_r)\to a_1m_1+\cdots+a_rm_r,$$

则 f 是 A^r 到 M 的一个 A 模同态且为满同态.

于是 M 同构于半单模 A^r 的一个商模. 由引理 3.3.2 知 M 是半单的，从而 A 是半单代数. 反之，由定义直接可得.

定理 3.3.4 设 A 是一个半单代数，A 作为 A 模，可设

$$A\cong S_1\oplus\cdots\oplus S_r,$$

其中 S_i 是 A 的单子模，$1\leqslant i\leqslant r$，则任何一个单 A 模同构于某个 S_i.

证明 设 S 是一个单 A 模，固定某个 $0\neq s\in S$，令 $\varphi(a)=as$，其中 $a\in A$，则 φ 是 A 到 S 的一个 A 模同态，因为 S 是单模，故 φ 是满射. 对每个 i 来说，令 $\varphi_i: S_i\to S$ 是 φ 在 S_i 上的限制，若对所有的 i 来说，$\varphi_i=0$，则必有 $\varphi=0$. 这与 $\varphi\neq 0$ 相矛盾，故必存在某个 i

使 $\varphi_i\neq 0$，由 Schur 引理可知，$\varphi_i: S_i\to S$ 是同构映射.

定理 3.3.5　设 A 是半单代数，$S_1,\cdots,S_r$ 是所有不同构的单 A 模，即每一个 A 模恰好同构于某个 S_i，设 M 是一个 A 模，不妨设为 $M\cong n_1S_1\oplus\cdots\oplus n_rS_r$，其中 n_i 为非负整数，$1\leqslant i\leqslant r$，则 n_i 是唯一确定的.

证明　对于 A 模 $n_1S_1\oplus\cdots\oplus n_rS_r$ 来说，存在一个有 $n_1+\cdots+n_r$ 项的合成列，在这个合成列中，每个 S_i 作为合成因子出现 n_i 次，由模的 Jorder-Holder 定理，结论成立.

下面我们将分类所有的半单代数. 首先我们证明某一类代数的半单性，然后我们证明所有的半单代数属于这个类中.

设 D 是一个有限维 F 代数，$M_n(D)$ 表示分量在 D 中的所有 $n\times n$ 矩阵组成的集合，则 $M_n(D)$ 是一个 $n^2\dim_F D$ 维的 F 代数，称为 D 上的矩阵代数. 令 $E_{ij}(a)$ 表示 (i,j) 位置为 a、其余位置为零的矩阵，D^n 表示元素在 D 中且长度为 n 的列向量构成的集合，则对于矩阵乘法来说，D 是一个 $M_n(D)$ 模.

定理 3.3.6　设 D 是一个可除代数，$n\in\mathbf{N}$，则单 $M_n(D)$ 模同构于 D^n；$M_n(D)$ 作为 $M_n(D)$ 模，它同构于 n 个 $M_n(0)$ 模 D^n 的直和. 特别地 $M_n(D)$ 是半单代数.

证明　D^n 的一个非零子模 N 必含有一个非零向量 v，因而对某个 j 来说，必有一个非零元素，在 u 的第 j 个位置. 用 $E_{ij}(x^{-1})$ 左乘 v，则 N 含有第 j 个标准基向量 v_j，即第 j 个位置为 1、其余位置为零的 n 维列向量. 用适当的置换矩阵左乘 v_j，则易得对每个 $1\leqslant j\leqslant n$，N 含有所有标准基向量. 因而 D^n 是 D^n 的唯一的非零 $M_n(D)$ 子模，即 D^n 是单 $M_n(D)$ 模.

对每个 $1\leqslant k\leqslant n$，令 C_k 表示非零元素在第 k 列，其余列均为零的 $n\times n$ 矩阵构成的集合，则 C_k 是 $M_n(D)$ 子模.

显然，$M_n(D)$ 作为 $M_n(D)$ 模，我们有 $M_n(D)\cong\bigoplus_{k=1}^n C_k$.

又 C_k 作为 $M_n(D)$ 模，它同构于 D^n，由引理 3.3.3 得 $M_n(D)$ 是半单代数. 又由定理 3.3.4 知，在同构意义下，D^n 是唯一的单 $M_n(D)$ 模.

引理 3.3.7　单代数一定是半单代数.

证明　令 A 是一个单代数，把 A 看作是一个 A 模，令 Σ 是 A 的所有单子模的和，S 是 A 的一个单子模，对于 $s\in S$，$a\in A$，令 $\varphi: s\longmapsto sa$，则 φ 是 S 到 Sa 的一个模同态. 于是 $Sa=0$ 或 Sa 是一个单模，无论哪种情况，均有 $Sa\subseteq\Sigma$. 由此得 Σ 是 A 的一个右理想，从而是 A 的一个理想. 但 A 是单代数且 $\Sigma\neq 0$，故 $A=\Sigma$，也即 A 是一些单 A 模的和，由引理 3.3.1 和 3.3.3 得 A 是半单代数.

定理 3.3.8　设 D 是可除代数，$n\in\mathbf{N}$，则 $M_n(D)$ 是单代数.

证明　设 $0\neq M\in M_n(D)$，我们需证明由 M 生成 $M_n(D)$ 的主理想 J 就是 $M_n(D)$ 本身，为此只要证明 J 含有每一个 $E_{ij}(1)$ 即可. 因为 $M\neq 0$，必有 $1\leqslant r,s\leqslant n$ 使得 M 的

(r,s)位置的元素不为零,把这个元素记为x,容易验证

$$E_{ss}(1)=E_{sr}(x^{-1})ME_{ss}(1)\in J.$$

令$1\leqslant i,j\leqslant n$,$w$和$w'$分别是对应于对换$(i,s)$与$(s,j)$的置换矩阵,则$E_{ij}(1)=wE_{ss}(1)w'\in J$.这就完成了证明.

引理 3.3.9 设$B=B_1\oplus\cdots\oplus B_n$是$n$个代数的直和,则$B$的理想恰如$J_1\oplus\cdots\oplus J_n$这种形状,其中$J_i$是$B_i$的理想,$1\leqslant i\leqslant n$.

证明 设J是B的理想,对$\forall\ i$,令$J_i=J\cap B$,则

$$\oplus_{k=1}^n J_i\subseteq J.\ b=b_1+\cdots+b_n,$$

其中$b_i\in B_i$,固定某个i,令$e_i=0+\cdots+0+1+0+\cdots+0$,其中1为$B_i$的单位元,则$b_i=be_i\in J\cap B_i=J_i$,故$b\oplus_{k=1}^n J_i$,这就证明$J$具有所希望的形式.

反之,易证具有$J_1\oplus\cdots\oplus J_n$这种形状的集合是$B$的理想.

定理 3.3.10 设$r\in\mathbf{N}$,$1\leqslant i\leqslant r$,D_i是F上的可除代数,对于$n_i\in\mathbf{N}$,令$B_i=M_n(D)$,设B是B_i的外直和,则B是半单代数且它恰有r个互不同构的B模以及2^r个理想且每个理想恰具有$\oplus_{j\in J}B_j$这种形状,其中$J\subseteq\{1,2,\cdots,n\}$.

证明 对每个i,由定理3.3.6知,$B_i=C_{i1}\oplus\cdots\oplus C_{in_i}$,其中$C_{ij}(1\leqslant j\leqslant n)$是相互同构的单$B_i$模.令$(b_1,\cdots,b_r)m=b_im$,则$C_{ij}$也作成一个$B$模.显然,如果$C_{ij}$作为$B_i$模是单模(半单模),则它作为$B$模也是单模(半单模).于是作为$B$模,$B\cong\oplus_{j,i}C_{ij}$,由引理3.3.3知$B$是半单代数.又由定理3.3.4知,任何一个单$B$模同构于某个$C_{ij}$.但是作为$B$模来说,$C_{ij}\cong C_{kl}$,当且仅当$i=k$,故恰有$r$个互不同构的单$B$模.关于理想的结论,由定理3.3.8和引理3.3.9即得.

上面我们证明了可除代数上矩阵代数的直和是半单代数.下面将证明,这个逆也是对的,即任何一个半单代数都同构于可除代数上矩阵代数的直和.

首先我们建立自同态代数与反代数之间的密切联系.

引理 3.3.11 设B是一个代数,则$B^{op}\cong\mathrm{End}_B(B)$.

证明 设$\varphi\in\mathrm{End}_B(B)$,$a=\varphi(1)$,则对$\forall\ b\in B$,$\varphi(b)=b\varphi(1)=ba$,也即$\varphi$是$B$的右乘变换定义的自同态,记$\varphi=f_a$,于是我们有$\mathrm{End}_B(B)=\{f_a\mid a\in B\}$,这就意味着$\mathrm{End}_B(B)$与$B$之间一一对应.

为完成证明,只需证对$\forall\ a,b\in B$有$f_a f_a=f_{a\cdot b}$,任取$x\in B$,我们有$(f_a f_a)(x)=f_a(xb)=xba=f_{ba}(x)=f_{a\cdot b}(x)$,这就完成了证明.

引理 3.3.12 设$S_1,\cdots,S_r$是不同的单A模,对每个i,$1\leqslant i\leqslant r$,令U_i是有限个S_i的直和,$U=U_1\oplus\cdots\oplus U_r$,则

$$\mathrm{End}_A(U)\cong\mathrm{End}_A(U_1)\oplus\cdots\oplus\mathrm{End}_A(U_r)J.$$

证明 设$\varphi\in\mathrm{End}_A(U)$,固定某个$i$,则$U_i$的每个合成因子同构于$S_i$.由模的

Jordan-Holder 定理知，$\varphi(U_i)$的每个合成因子也同构于 S_i.

首先我们证明 $\varphi(U_i)\subseteq U_i$. 假设 $\varphi(U_i)$不包含在 U_i 中，在自然映射下，$\varphi(U_i)$在U/U_i中的像是一个非零子模，且有 S_i 作为它的一个合成因子. 另一方面，由题设可知，U/U_i的合成因子恰好是那些 S_j，其中 $i\neq j$，因而 U/U_i，的子模不可能有 S_i 作为其合成因子. 这就得出 $\varphi(U_i)\subseteq U_i$. 令 φ_i 是 φ 在 U_i 上的限制，则 $\varphi_i\in \mathrm{End}_A(U_i)$. 作 $\mathrm{End}_A(U)$到 $\mathrm{End}_A(U_i)\oplus\cdots\oplus\mathrm{End}_A(U_r)$的映射

$$T:\varphi\longmapsto(\varphi_1,\cdots,\varphi_r),$$

则易证 T 是 A 模单同态.

再证 T 是满射即可. 设$(\varphi_1,\cdots,\varphi_r)\in\mathrm{End}_A(U_i)\oplus\cdots\oplus\mathrm{End}_A(U_r)$，任取 $x\in U$，则 $x=x_1+\cdots+x_r$，其中 $x_i\in U_i$.

令 $\varphi(x)=\varphi_1(x=1)+\cdots+\varphi_r(x_r)$，则易验证 $\varphi\in\mathrm{End}_A(U)$且 $T(\varphi)=(\varphi_1,\cdots,\varphi_r)$，故 T 是满射.

引理 3.3.13 若 S 是一个单 A 模，则对任意的 $n\in\mathbf{N}$，都有

$$\mathrm{End}_A(nS)\cong M_n(\mathrm{End}_A(S)).$$

证明 把 nS 的元看作分量为 S 中元的 n 维列向量. 令 $\Phi=(\varphi_{ij})\in M_nL(\mathrm{End}_A(S))$，定义 nS 到 nS 的映射 $T(\Phi)$，

$$T(\Phi)\begin{pmatrix}s_1\\ \vdots\\ s_n\end{pmatrix}=\begin{pmatrix}\phi_{11}&\cdots&\phi_{1n}\\ \vdots& &\vdots\\ \phi_{n1}&\cdots&\phi_{nn}\end{pmatrix}\begin{pmatrix}s_1\\ \vdots\\ s_n\end{pmatrix}=\begin{pmatrix}\phi_{11}(s_1)+&\cdots&+\phi_{1n}(s_n)\\ &\vdots& \\ \phi_{n1}(s_1)+&\cdots&+\phi_{nn}(s_n)\end{pmatrix}$$

因为每个 φ_{ij}是 A 模同态，容易验证对$\forall\ a\in A, s,t\in nS$，都有

$$T(\Phi)(as+t)=a[T(\Phi)(s)]+T(\Phi)(t),$$

因而 $T(\Phi)\in\mathrm{End}_A(nS)$. 可以验证以上定义的

$$T: M_n(\mathrm{End}_A(S))\to\mathrm{End}_A(nS)$$

是一个代数单同态. 只需证 T 是满射即可.

令 $\psi\in\mathrm{End}_A(nS)$，对$\forall\ 1\leqslant i,j\leqslant n$，定义 S 到 S 的映射

$$\psi_{ij}:\psi\begin{pmatrix}s\\0\\ \vdots\\0\end{pmatrix}=\begin{pmatrix}\psi_{11}(s)\\ \psi_{21}(s)\\ \vdots\\ \psi_{n1}(s)\end{pmatrix},\cdots,\psi\begin{pmatrix}0\\ \vdots\\0\\s\end{pmatrix}=\begin{pmatrix}\psi_{1n}(s)\\ \psi_{2n}(s)\\ \vdots\\ \psi_{nn}(s)\end{pmatrix}$$

容易验证每个 $\psi_{ij}\in\mathrm{End}_A(S)$，令 $\Psi=(\psi_{ij})$，则 $\Psi\in M_n(\mathrm{End}_A(S))$，于是 $T(\Psi)=\psi$，这就证明了 T 是满射.

如果 S 是一个单 A 模，由 Schur 引理直接可得 $\mathrm{End}_A(S)$是一个可除代数. 进一步地，代数闭域上的代数 $\mathrm{End}_A(S)$有更具体的结构.

引理 3.3.14 设 F 是代数闭域，S 是一个单 A 模，则 $\mathrm{End}A(S)\cong F$.

证明 设 $\varphi\in\mathrm{End}_A(S)$，把 φ 看作为有限维 F 向量空间 S 上的 F 线性变换. 因为 F 是代数闭域，φ 在 F 中有一个非零特征根 λ_φ，设 I 是 $\mathrm{End}_A(S)$ 的恒等元，则 $\varphi-\lambda_\varphi I\in\mathrm{End}_A(S)$ 有非零的核，因而不是可逆的. 因为 $\mathrm{End}_A(S)$ 是可除代数，这就迫使 $\varphi=\lambda_\varphi I$. 可以验证，$\varphi\longmapsto\lambda_\varphi I$ 是 $\mathrm{End}_A(S)$ 到 F 的一个同构映射.

引理 3.3.15 设 B 是一个代数，则对 $\forall\ n\in\mathbf{N}$，都有 $M_n(B)^{op}\cong M_n(B^{op})$.

证明 设 $X\in M_n(B)^{op}$，令 $\psi(X)=X'$，其中 X' 为矩阵 X 的转置，容易看出 ψ 是 $M_n(B)^{op}$ 到 $M_n(B^{op})$ 的一一对应.

任取 $X=(x_{ij}),Y=(y_{ij})\in M_n(B)^{op}$，则对 $\forall\ i,j$，我们有

$$\begin{aligned}(\psi(X)\psi(Y))_{ij}&=\sum_{k=1}^{n}\psi(X)_{ik}\psi(Y)_{kj}=\sum_{k=1}^{n}X'_{ik}Y'_{kj}\\&=\sum_{k=1}^{n}x_{ki}y_{jk}=\sum_{k=1}^{n}y_{jk}x_{ki}=(YX)_{ji}\\&=(YX)'_{ij}=(XY)'_{ij}=\psi(XY)_{ij},\end{aligned}$$

这表明

$$\psi(XY)=\psi(X)\psi(Y),$$

由此可知 ψ 是一个代数同态.

有了以上的准备工作，现在我们可以给出半单代数的结构定理.

定理 3.3.16 代数 A 是半单的 $\Leftrightarrow A$ 同构于可除代数上矩阵代数的直和.

证明 设 A 是半单代数，则 $A=U_1\oplus\cdots\oplus U_r$，其中 U_i 是 n_i 个单 A 模 S_i 的直和，当 $i\neq j$ 时，S_i 与 S_j 不同构.

我们有

$$\begin{aligned}A^{op}&\cong\mathrm{End}_A(A)\cong\mathrm{End}_A(U_1)\oplus\cdots\oplus\mathrm{End}_A(U_r)\\&\cong\mathrm{End}_A(n_1S_1)\oplus\cdots\oplus\mathrm{End}_A(n_rS_r)\\&\cong M_{n_1}(\mathrm{End}_A(S_1))\oplus\cdots\oplus M_{n_r}(\mathrm{End}_A(S_r)),\end{aligned}$$

于是我们有

$$\begin{aligned}A&\cong[M_{n_1}(\mathrm{End}_A(S_1))\oplus\cdots\oplus M_{n_r}(\mathrm{End}_A(S_r))]^{op}\\&\cong M_{n_1}(\mathrm{End}_A(S_1))^{op}\oplus\cdots\oplus M_{n_r}(\mathrm{End}_A(S_r))^{op}\\&\cong M_{n_1}(\mathrm{End}_A(S_1)^{op})\oplus\cdots\oplus M_{n_r}(\mathrm{End}_A(S_r)^{op}).\end{aligned}$$

因为一个单模的自同态代数是可除代数，可除代数的反代数也是可除代数. 由此得知，任意一个半单代数同构于可除代数上矩阵代数的直和.

反之，由定理 3.3.10 可得.

定理 3.3.17 代数 A 是单代数 $\Leftrightarrow A$ 同构于某个可除代数上的矩阵代数.

证明　设 A 是单代数，由引理 3.3.7 知，A 是半单的. 再由定理 3.3.16 得 A 同构于可除 F 代数上 r 个矩阵代数的直和. 但由定理 3.3.10 知，A 恰有 2^r 个理想，又 A 是单代数，故 A 恰仅有 2 个理想，故我们有 $r=1$. 因而任何单代数同构于某个可除代数上的矩阵代数. 由定理 3.3.8 得出定理的另一面.

代数闭域上的半单代数有更简明的结构.

定理 3.3.18　设 F 是代数闭域，A 是 F 上的半单代数，则 A 同构于 F 上的矩阵代数的直和.

问题 3.3

1. 设 $n\in\mathbf{N}$，令 $yn(F)$ 是 $n\times n$ 上三角矩阵构成的代数，$V_n(F)$ 是 F 上 n 维列向量集合，证明：$V_n(F)$ 关于向量的加法与矩阵乘法构成 $T_n(F)$ 模，且它有唯一的合成列使得每一个单 $T_n(F)$ 模作为合成因子在这个合成列中恰好出现一次.

2. $T_n(F)$，$V_nF(F)$ 如上题所设，证明：$T_n(F)$ 模 $T_n(F)$ 同构于 $V_n(F)$ 的所有非零子模的直和.

3. 设 U 是一个 A 模，令 $n\in\mathbf{N}$，U^n 是元素在 U 中的 n 维列向量组成的集合，与第 1 题的运算相同，U^n 作成一个 $M_n(A)$ 模. 证明：U 是一个单 A 模当且仅当 U^n 是一个单 $M_n(A)$ 模.

4. 对任意的 A 模 U，V，都有 $\mathrm{Hom}_A(U,V)\cong\mathrm{Hom}_{M_n(A)}(U^n,V^n)$.

5. 证明：A 是单 A 模当且仅当 A 是可除代数.

6. 设 B 是一个有限维 F 代数，不一定有单位元，证明：如果 B 是一个单代数且其乘法运算不恒为零，则 B 同构于某个可除代数上的矩阵代数.

Jordan 小传

若尔当(M. E. C. Jordan)，法国数学家，1838 年 1 月 5 日生于里昂. 1855 年以第一名的成绩进入巴黎综合工科学校. 毕业后进入矿业学校，以后任工程师至 1885 年. 从 1873 年至 1912 年，Jordan 同时在巴黎综合工科学校和法兰西学院任教. 1881 年被选为法兰西科学院院士.

在代数、几何、分析、拓扑学以及数学基础方面均有重要贡献. 以他的名字命名的概念有：矩阵论中的若尔当典范型、拓扑学中的若尔当定理、群论中的若尔当—赫尔德(O. L. Holder)定理和若尔当代数等.

Jordan 在 1870 年发表的《置换与代数方程论》是一部经典著作，其中首次将由伽罗瓦创建的确定多项式的根式解的理论(即伽罗瓦理论)进行了清晰和完整的论述，并特别研究了线性变换群、可解群及其在代数和几何上的应用. 在这本书中，Jordan 还首

次将交换群称为 Abel 群. 虽然群这一术语是伽罗瓦引入的,但正是 Jordan 的著作才使得该术语为广大数学家所接受. 他的另一影响巨大的书是《分析教程》,这是第一部严密的分析著作,特别是提出了有名的 Jordan 定理.

Jordan 于 1922 年 1 月 22 日在巴黎逝世.

§3.4 有限结合代数的表示

有限群的表示理论是群和代数的一个重要分支,它在群论本身以及在物理、化学等学科都有着广泛的应用. 有限群的表示理论大致可分为两类,一为常表示理论,一为模表示理论. 前者在有限群的发展中起了很大作用,后者对于著名的有限单群分类问题的解决提供了有力的工具.

一个抽象的研究对象,人们总希望用一个具体的研究对象表示它. 例如,任意一个域 F 上的 n 维向量空间都可用 n 元序组作成的向量空间 F^n 来表示;任意一个环可用一个交换群的自同态作成的环表示,类似地,任意一个结合代数可用一个向量空间的线性变换或矩阵作成的代数来表示.

定义 3.4.1 设 A 是域 F 上有限维结合代数,V 是 F 上 n 维向量空间,称代数同态 $\varphi: A\to M_n(F)$ 为 A 的一个矩阵表示,

称代数同态 $\varphi: A\to \mathrm{End}_F(V)$ 为 A 的一个线性表示,有时简称为表示. V 称为表示空间,n 称为表示的级.

定义 3.4.2 两个矩阵表示 φ_1,φ_2 称为等价的,如果它们的级数相同,且存在一个可逆矩阵 S,使得 $\varphi_1(a)=S(\varphi_2(a))S^{-1},a\in A$. 两个线性表示 φ_1,φ_2 称为等价的,若存在向量空间的同构 $\psi: V_1\to V_2$,使得 $\varphi_2(a)=\psi(\varphi_1(a))\psi^{-1},a\in A$.

易证,等价是表示之间的一个等价关系.

我们知道,域 F 上 n 维向量空间 V 的所有线性变换关于变换的加法和数乘作成一个 F 上的 n^2 维向量空间,F 上所有 $n\times n$ 矩阵关于矩阵的加法和数乘构成一个向量空间. 它们是同构的. 同一个线性变换在不同基下的矩阵是相似的. 于是,等价的矩阵表示对应于等价的线性表示,从本质上看,它们是完全相同的.

下面我们给出表示的另一个描述,它使得我们对代数的表示的研究可通过代数上的模来研究.

设 φ 是代数 A 的一个表示,$\varphi(a)=T_a\in M_n(F),a\in A$,令 V 是 F 上一个 n 维向量空间,$v_1,\cdots,v_n$ 是 V 的一个基.

对于 $x\in V$,则

$$x=k_1v_1+\cdots+k_nv_n,k_1,\cdots,k_n\in F,$$

令

$$ax=(v_1,\cdots,v_n)T_a\begin{pmatrix}k_1\\ \vdots\\ k_n\end{pmatrix}.$$

因为 φ 是 A 到 $M_n(F)$ 的一个代数同态，直接验证可知下列等式成立：

$$a(x+y)=ax+ay,a(kx)=(ak)x=k(ax),$$
$$(a+b)x=ax+bx,(ab)x=a(bx),$$

其中 $a,b\in A,x,y\in V,k\in F$.

这说明 A 中元通过 φ 可定义为向量空间 V 的一个线性变换，即存在 $A\times V$ 到 V 的映射满足上述性质，这启发我们引出下列重要概念.

定义 3.4.3　设 A 是域 F 上有限维结合代数，V 是域 F 上有限维向量空间，我们说 V 是一个代数 A 的代数模，或代数 A 的表示空间，若存在一个 $A\times V$ 到 V 的映射 $(a,v)\longmapsto v$ 满足下列性质：

(1)对$\forall\ v\in V$ 有 $1v=v$；

(2)对$\forall\ a\in A,u,v\in V$ 有 $a(u+v)=au+av$；

(3)对$\forall\ a,b\in A,v\in V$ 有 $(a+b)v=av+bv$；

(4)对$\forall\ a,b\in A,v\in V$ 有 $a(bv)=(ab)v$；

(5)对$\forall\ a\in A,k\in F,v\in V$ 有 $a(kv)=(ak)v=k(av)$.

代数 A 的两个代数模 V 和 V'，称为同构的，如果有 V 到 V' 的一个双射 $\varphi:v\longmapsto v'$，使对$\forall\ v_1,v_2,v\in V,a\in A,k\in F$ 都有

$$(v_1+v_2)'=v'_1+v'_2,(av)'=av',(kv)'=kv'.$$

相应地可定义代数模的同态、子模、商模等概念. 相应的同态基本定理，第一、二同构定理对于代数模也是成立的.

下面我们讨论代数的表示与代数模之间的关系. 上面的讨论说明代数 A 的一个表示可定义代数 A 的一个代数模. 反过来，给定代数 A 的代数模 V，也可以按如下方法得到代数 A 的一个表示.

任取 V 在 F 上的一个基 $\{v_1,\cdots,v_n\}$，对$\forall\ a\in A$，我们有 $av_i=\Sigma k_{ij}v_j\in F$，令 $T_a=(a_{ij})$，则易验证 $\varphi:a\longmapsto T_a$ 是 A 到 $M_n(F)$ 的一个代数同态，即 φ 是代数 A 的一个表示.

定理 3.4.1　代数 A 的两个表示等价$\Leftrightarrow$它们对应的代数模同构.

证明　设 φ_1,φ_2 是代数 A 的两个互相等价的矩阵表示，而 V_1,V_2 分别为 φ_1,φ_2 所对应的代数模，首先证明必要性，即存在域 F 上一个 n 阶可逆矩阵 S 使得

$$\varphi_1(a)=S(\varphi_1(a))S^{-1},\ a\in A.$$

根据以上讨论,表示 φ_i 所对应的代数模 V_i 的数乘运算定义为

$$a\begin{pmatrix}v_{i1}\\ \vdots\\ v_{in}\end{pmatrix}=(v_{i1},\cdots,v_{in})\varphi_i(a),i=1,2.$$

其中 $v_{i1},\cdots,v_{in}$ 是向量空间 V_i 的基,$i=1,2,n$ 为表示 φ_1,φ_2 的相同的级数.

令

$$\psi\begin{pmatrix}v_{11}\\ \vdots\\ v_{1n}\end{pmatrix}=S\begin{pmatrix}v_{21}\\ \vdots\\ v_{2n}\end{pmatrix}$$

则 ψ 是向量空间 V_1 到 V_2 的同构对应,可验证 ψ 也是代数模 V_1 到 V_2 的同构对应,即等价表示对应的代数模是同构的.

下面再看充分性,设 V_1 与 V_2 是同构的,Ψ 是其同构映射所对应的矩阵,$\{v_{i1},\cdots,v_{in}\}$ 是 $V_i(i=1,2)$ 的基,则

$$\{v_{11}^{\psi},\cdots,v_{1n}^{\psi}\}=\{v_{i1},\cdots,v_{in}\}\psi$$

是代数模 V_2 的一个基,对于 $a\in A,\varphi_1(a)\in M_n(F)$ 有

$$a\begin{pmatrix}v_{11}\\ \vdots\\ v_{1n}\end{pmatrix}=(v_{11},\cdots,v_{1n})\varphi_1(a),$$

则可验证

$$a\begin{pmatrix}v_{11}^{\psi}\\ \vdots\\ v_{1n}^{\psi}\end{pmatrix}=(v_{11}^{\psi},\cdots,v_{1n}^{\psi})\psi^{-1}\varphi_1(a)\psi$$

于是 $\psi\varphi_1(a)\psi^{-1}\in M_n(F)$.

由高等代数知识可知,同一线性变换在不同基下的矩阵是相似的,所以存在可逆矩阵 T,使得 $\psi\varphi_1(a)\psi^{-1}=T\varphi_2(a)T^{-1}$,即说明表示 φ_1 和 φ_2 是等价的.

定义 3.4.4 域 F 上代数 A 的一个表示 φ 称为忠实的,若 $\varphi:A\to\mathrm{End}_F(V)$(或 $\varphi:A\to M_n(F)$)是一个代数单同态.

代数 A 的代数模 V 称为忠实的,若对任意的 $a\in A$,由 $aV=0$ 必有 $a=0$.

由定义易知,忠实代数模所决定的表示是忠实的,而忠实表示所对应的代数模也是忠实的.

代数 A 本身可看作代数 A 的代数模,这是因为 A 是域 F 上的向量空间,而数乘运算就规定为 A 的乘法运算,可知 A 是 A 上的代数模.

定义 3.4.5 A 称为代数 A 的正则代数模,它所决定的表示称为代数 A 的正则表

示.

由 A 有单位元可知,A 的正则代数模是忠实的,这是因为若 $aA=0$,必有 $1a=0$,即 $a=0$. 这样 A 的正则表示是 A 的忠实表示,亦即有单位元的 n 维代数 A 可看作 $M_n(F)$ 的一个子代数. 这类似于群论中的 Cayley 定理.

定义 3.4.6　代数 A 的一个表示 ψ 称为可约的,若存在与 ψ 等价的一个表示 φ,具有性质

$$\varphi(a)=T_a=\begin{pmatrix}T_{11} & S_{12}\\ 0 & T_{22}\end{pmatrix},a\in A,$$

其中 T_{11},T_{22} 分别是不全为零的 $n_1\times n_1,n_2\times n_2$ 矩阵,$n_i>0,i=1,2$,否则就说表示 ψ 是不可约的或既约的.

代数 A 的一个代数模 V 称为不可约的或既约的,若 V 的子模只有零和 V 自身,否则就说 V 是可约的. 非零既约代数模称为单代数模.

这些概念与前几节的有关概念是一致的,我们有下面的结果,

定理 3.4.2　代数 A 的表示 φ 是既约的$\Leftrightarrow\varphi$ 对应的代数模是既约的.

证明　首先我们看到,若代数 A 的一个矩阵表示 φ 是可约的,不妨设

$$\varphi(a)=T_a=\begin{pmatrix}T_{11} & S_{12}\\ 0 & T_{22}\end{pmatrix},a\in A,$$

其中 T_{11},T_{22} 分别是不全为零的 $n_1\times n_1,n_2\times n_2$ 矩阵,$n_i>0,i=1,2,n=n_1+n_2$ 表示 φ 的级数,直接验证可知

$$\varphi_1:a\longmapsto T_{11},\varphi_2,a\longmapsto T_{22}$$

是代数 A 的两个级数比 n 低的表示.

现在设可约表示 φ 所对应的代数模为 $V,v_1,,\cdots,v_n$ 是 V 作为 F 向量空间的一个基. 其数乘运算为

$$a\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}=T_a\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}$$

注意到 T_a 的形状,我们看到由 $v_{n_1+1},\cdots,v_n$ 生成的 n_2 维子空间 V_2 必是 V 的代数子模,这是因为

$$a\begin{pmatrix}v_{n_1+1}\\ \vdots\\ v_n\end{pmatrix}=(0,T_{22})\begin{pmatrix}v_1\\ \vdots\\ v_n\end{pmatrix}=T_{22}\begin{pmatrix}v_{n_1+1}\\ \vdots\\ v_n\end{pmatrix}$$

则 V_2 就是与 φ_2 相应的一个代数模,即可约表示对应的代数模是可约的.

设代数模 V 是可约的,V_2 是它的真子模,利用 V_2 按下面的方法可得一个代数模:

取向量空间 V 关于子空间 V_2 的商空间 $\bar{V}=V/V_2$，其元素为 $\bar{v}=v+V_2$，规定乘法运算：$a\bar{v}=\overline{av}$，$\bar{v}\bar{V}$，$a\in A$.

直接验证可知 $\bar{V}$ 关于这个运算是一个代数模，称为代数模 V 关于 V_2 的代数商模. 取代数商模 V/V_2 的 F 基 $\bar{v}_1,\cdots,\bar{v}_n$，则

$$a\begin{pmatrix}\bar{v}_1\\ \vdots\\ \bar{v}_n\end{pmatrix}=\begin{pmatrix}a\,\bar{v}_1\\ \vdots\\ \bar{a}\,\bar{v}_n\end{pmatrix}=T_{11}\begin{pmatrix}\bar{v}_1\\ \vdots\\ \bar{v}_n\end{pmatrix}$$

即商模 V/V_2 是与表示 φ_1 相对应的代数模.

总之，若可约表示 φ 相对应的代数模是 V，则可约表示 φ 所导出的表示 φ_2，φ_1 分别相对应于 V 的代数子模 V_2 与商模 V/V_2.

代数表示论的基本问题之一是决定代数 A 在域 F 上的所有不等价的不可约表示，这等价于决定所有互不同构的不可约 A 模，一般来说，决定结合代数 A 的所有不可约表示是非常困难的，但对代数闭域上的半单代数而言，由定理 3.3.18 知，这个问题已完全解决.

问题 3.4

1. 四元数除环作为实数域上的代数，给出这个代数关于基 $1,i,j,k$ 的正则表示，这个表示可约吗？

2. 给出全矩阵代数关于基 e_{ij} 的正则表示，这个表示可约吗？

§3.5　群表示初步

1. 群的表示

若群 G 与正则 $n\times n$ 矩阵群 $\{\Gamma\}$ 同态，则称 $\{\Gamma\}$ 为群 G 的一个 n 维线性表示，即 $\forall\ g_{ia}\in G(a=1,2,\cdots,m)$，有映射

$$f:g_{i1},g_{i2},\cdots g_{im}\to\Gamma(g_i),\quad \Gamma(g_i)\in\{\Gamma\},$$

并且 f 是保持乘法的：$\forall\ g_{ij}\cdot g_{jm}\xrightarrow{f}\Gamma(g_i)\Gamma(g_j)$. 当 $m=1$ 且映射为可逆时，映射为同构的，称表示为忠实的；当 $m>l$ 时，映射为同态的，称表示为非忠实的，此时表示只能反映群的大致结构，或只能反映 G 与同态核 N 的商群 G/N 的群结构.

2. 表示的基

上面定义的表示，实际上是群元在某个基矢组下的表示，离开基矢组，表示无从谈

起.基矢组所张成的线性空间,称为表示空间.考察群元如何作用于表示空间中的矢量,可从两种观点分析.

(1)主动观点.群元只对矢量投影进行变换,不影响基矢.设$\forall X \in L_n$,为n维表示空间,则利用一组正交归一基矢组$\{b_i\}(i=1,2\cdots n)$,对其展开:$X=\sum_{i=1}^{n} X_i b_i$.在群元g_σ的作用下,有

$$x \xrightarrow{g_\sigma} x' = g_\sigma x = g_\sigma(\sum_{i=1}^{n} x_i b_i) = \sum_i b_i \cdot g_\sigma x_i,$$

矢量分量x_i变化的方式为

$$x_i = (b_i, x) \xrightarrow{g_\sigma} x' = (b_i, x') = (b_i, g_\sigma x) = \sum_{j=1}^{n} (b_i, g_\sigma b_j) x_j = \sum_{j=1}^{n} \Gamma(g_\sigma)_{ij} x_j$$

其中$\Gamma(g_\sigma)_{ij}(i,j=1,2,\cdots,n)$为表示的矩阵元,符号$(\cdot,\cdot)$表示内积,并且在运算中用到正交归一关系:$(b_i,b_j)=\delta_{ij}(i,j=1,\cdots,n)$.

将上式写成矩阵形式,简记为$x \xrightarrow{g_\sigma} x' = \Gamma(g_\sigma)x$.

(2) 被动观点.群元只对基矢作用,不影响矢量.此时基矢组$\{b_1,b_2,\cdots,b_n\}$在群元g_σ作用下,有$b_i \xrightarrow{g_\sigma} b'_i = g_\sigma b_i$.引入投影算符$P_j^m x = x_j b_j(m \geqslant 1)$(等幂性);

$$\sum_{j=1}^{n} P_j x = EX \Rightarrow \sum_{j=1}^{n} P_j = E(\text{完备性条件}),$$

将此式作用于上式两边,注意到E为$n \times n$单位矩阵,有

$$Eb' = b' = \sum_{j=1}^{n} b_j (b_j, g_\sigma b_i) \equiv \sum_{j=1}^{n} b_j \Gamma(g_\sigma)_{ji}.$$

写成矩阵形式:

$$(b_1,b_2,\cdots,b_n) \xrightarrow{g_\sigma} (b'_1,\cdots,b'_n) = (b_1,\cdots,b_n)\begin{bmatrix} \Gamma(g_\sigma)_{11} & \cdots & \Gamma(g_\sigma)_{1n} \\ \vdots & & \vdots \\ \Gamma(g_\sigma)_{n1} & \cdots & \Gamma(g_\sigma)_{nn} \end{bmatrix}$$

即$b=b\Gamma(g_\sigma)$.

但是无论按主动观点还是被动观点,在群元$\{g_\sigma\}$的作用下,其物理结果应是相同的.试看下面例子.

例 3.5.1　设$L_n=E_3$,讨论矢量x在g_σ作用下的变化$x \xrightarrow{g_\sigma} x'(x=\sum_{i=1}^{3} x_i b_i)$,主动$x'=\sum_{i=1}^{3} x'_i b_i = \sum_{i,j=1}^{3} \Gamma(g_\sigma)_{ij} x_j b_i$;被动$x'=\sum_{i=1}^{3} x'_i b'_i = \sum_{i,j=1}^{3} x_i b_j \Gamma(g_\sigma)_{ji}$.显然两者结果相同.

例 3.5.2　设 $L_z = -\mathrm{i}h\dfrac{\mathrm{d}}{\mathrm{d}\varphi}$ 为量子力学角动量投影算符，其本征函数为

$$L_z = -\mathrm{i}h\frac{\mathrm{d}}{\mathrm{d}\Psi}\Psi_m = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{\mathrm{i}m\Psi}(L_z\Psi = m\Psi_m).$$

讨论系统绕 Z 轴转动 α 角，则球坐标 φ 经历变换

$$\varphi \xrightarrow{R_\alpha} \varphi' = \varphi + \alpha, \qquad \varphi \xrightarrow{R_\alpha - 1} \varphi' = \varphi - \alpha.$$

引入标量函数的变换算符 P_R，表示在坐标变换下，

$$x \to x' = Rx, x = R^{-1}x',$$

相应地，函数形式变化为 $P_R\Psi(x) = \Psi'(x)$.

对于标量函数应有 $\Psi'(x') = \Psi(x)$，故

$$P_R\Psi(x') = \Psi'(x') = \Psi(x) = \Psi(R^{-1}x'),$$

即(上式坐标 x' 均改记为 x)$P_R\Psi(x) = \Psi(R^{-1}x)$，对于本例，

$$P_R\Psi_m(\varphi) = \varphi_m(R^{-1}\varphi) = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{\mathrm{i}m(\varphi-\alpha)} = \mathrm{e}^{-\mathrm{i}m\alpha}\Psi_m(\varphi),$$

即 P_R 的作用等价于乘以因子 $\mathrm{e}^{-\mathrm{i}m\alpha}$，亦即 P_R 相当于算符 $\exp(-\mathrm{i}L_E\alpha)$.

容易证明，算符 P_R 的集合 $\{\exp(-\mathrm{i}L_E\alpha)\}$ 构成一个群，而且与坐标变换 $\{R\}$ 构成的群 G 同构，此时集合 $\{P_R\}$ 称为群 G 的线性实现.

例 3.5.3　量子力学中线性变换算符的变换规律. 设有线性算符

$$\Psi_B(x) = L(x)\Psi_A(x),$$

在坐标变换下 $x \xrightarrow{R} x' = Rx, x = R^{-1}x'$，波函数发生变化：

$$\Psi_A(x) \to \Psi'_A(x') = P_R\Psi_A(x'),$$

$$\Psi_B(x) \to \Psi'_B(x') = P_R\Psi_B(x').$$

但此时，

$$(x) \xrightarrow{R} L'(x'), \quad \Psi'_B(x') = L'(x')\Psi'_A(x'),$$

即

$$P_R\Psi_B(x') = P_R[L(x')\Psi_A(x')] = L'(x')P_R\Psi_A(x').$$

由于 Ψ_A 的任意性和 x' 的任意性，因而有

$$L'(x) = P_RL(x)P_R^{-1}.$$

注意，量子力学中物理量用厄米算符 L 表示. 我们已证明，如果 H 只是对称变换，则 P_R 对应守恒量，且 $[H, P_R] = 0$，式中 H 为系统的哈密尔顿量.

3. 表示的特征标

特征标即为表示矩阵的对角元之和，即

$$\chi_r(g_a)=\sum_{i=1}^{n}(g_i)=T_r[\Gamma(g_a)],$$

其中符号 $T_r[\cdot]$ 表示矩阵的迹.

特征标的一个重要性质是,同一表示中同一共轭类的群元的特征标相等. 注意到逆元素的表示矩阵必为该元素表示矩阵的逆阵,即

$$\Gamma(g_a^{-1})=\Gamma^{-1}(g_a).$$

这一性质极易验证:

$$T_r[\Gamma(g_a^{-1})\Gamma(g_\beta)\Gamma(g_a)]=T_r[\Gamma^{-1}(g_a)\Gamma(g_\beta)\Gamma(g_a)]$$

由于求迹时诸矩阵次序可循环移动,故

$$T_r[\Gamma(g_\beta)\Gamma(g_a)\Gamma^{-1}(g)]=\Gamma[\Gamma(g_\beta)].$$

就是说,特征标是类函数.

若 $\{\Gamma(g_a)\}$ 为群 G 的 n 维表示,X 是 $n\times n$ 正则矩阵,则集合 $\{\Gamma(g_a)\}$ (其中 $\Gamma'(g_a)=X^{-1}\Gamma(g_a)X$),亦构成群 G 的一个 n 维表示,称为 $\{\Gamma(g_a)\}$ 表示的等价表示. 实际上,由

$$\begin{aligned}\Gamma'(g_a)\Gamma'(g_\beta)&=(X^{-1}\Gamma(g_a)X)(X^{-1}\Gamma(g_\beta)X)\\&=X^{-1}\Gamma(g_a)\Gamma(g_\beta)X=\Gamma'(g_ag_\beta)\end{aligned}$$

即可看出 $\{\Gamma'(g_a)\}$ 亦为群 G 的表示.

显然,如此可以构造许多等价表示. 容易验证这些等价表示彼此之间具有所谓的等价关系(相互性、传递性和自反性),形成互相等价的所谓表示类. 群表示论的中心课题就是找到群的全部表示. 现在问题简化为寻找群的所有不等价表示类,每类表示只须找到一个表示就可以了. 显然,相应同一群元的诸等价表示的特征标相等.

在同一等价表示类中出现多种形式,实质上可以说是产生于表示空间的基底变换. 设矢量 $x,y\in L_n$,且 $y=\Gamma(g_a)x$. 当对基底进行变换时,

$$b'_i=b_iX_{ij}(i,j=1,\cdots,n),$$

由线性代数易知,对于新基底:

$$y'=\Gamma(g_a)x',$$

其中

$$y'=Xy,x'=Xx,\Gamma'(g_a)=X\Gamma(g_a)X^{-1}=(X^{-1})^{-1}\Gamma(g_a)X^{-1}.$$

在所有 n 维群的表示中,恒等元的表示矩阵是相应 n 维单位矩阵 $D(I)=E$;一切群都有一个一维平凡表示,或称恒等表示,就是任意 $g_i\in G,\Gamma(g_a)=1$.

对于矩阵群,其本身当然也是一个表示.

例 3.5.4 循环群 C_n.

$$C_n=(E,a,a^2,\cdots,a^{n-1},a^n=E)$$

令 $\omega=\exp(\frac{2\pi i}{n})$，此处 i 为虚数单位，令 $\Gamma(a)=\omega^p$，则 $\Gamma(E)=1$，其中整数 $0\leqslant p\leqslant n-1$.

显然，

$$\Gamma(a^m)=(\Gamma(a))^m=(\omega^p)^m\equiv\lambda^m(\lambda=\omega^p)(m=0,\pm1,\pm2,\cdots),$$

构成群 C_n 的一维表示 $\{\lambda^n\}$.

当 $\lambda=1$ 时，即 $p=0$，给出平凡表示，当 $\lambda\neq1$ 时，则表示不等价. 由于表示都是普通的数，等价表示必然相等. 但 p 只有 n 种选择，故此处给出 C_n 群 n 个不等价的一维表示(即给出 n 个不同 λ 值).

例 3.5.5　二面体群 D_n 为一操作群，如图 3.1 所示系循环群 C_n 的操作(用元素 $a=C_n^1$ 表示绕 O 点转动)，再加上对 Ox 轴的反射元素 $b:\theta\xrightarrow{b}-\theta$ 等所构成的集合：

$$D_n=\{I,a,a^2,\cdots,a^{n-1};ab,a^2b,\cdots,a^{n-1}b\}.$$

容易验证 D_n 构成一个群，称为二面体群. 显然有关系：

$$a^n=b^2=I,aba=b.$$

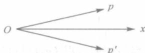


图 3.1

一维表示

$$\Gamma^{(1)}(a)=\Gamma^{(1)}(b)=\text{纯数},$$
$$\Gamma^{(1)}(a^n)=\Gamma^{(1)}(b^2)=\Gamma^{(1)}(E)=1,$$
$$\Gamma^{(1)}(aba)=\Gamma^{(1)}(b).$$

由此

$$[\Gamma^{(1)}(a)]^n=[\Gamma^{(1)}(b)]^2=1,\quad \Gamma^{(1)}(a)\Gamma^{(1)}(b)=1,$$

即

$$\Gamma^{(1)}(b)=\pm1,\quad (\Gamma(a))^n=1,\quad (\Gamma(a))^2=1.$$

当 n 为偶数时，有四种可能的选择：

$$\Gamma^{(1)}(a)=\Gamma^{(1)}(b)=1;\quad \Gamma^{(1)}(a)=\Gamma^{(1)}(b)=-1,$$
$$\Gamma^{(1)}(a)=1,\Gamma^{(1)}(b)=-1;\quad \Gamma^{(1)}(a)=-1,\Gamma^{(1)}(b)=1,$$

它们都是等价的，就是平凡表示.

当 n 为奇数时，有两种可能：

$$\Gamma^{(1)}(a)=\Gamma^{(1)}(b)=1;\quad \Gamma^{(1)}(a)-\Gamma^{(1)}(b)=1.$$

二维表示

引入符号 λ 与 ω，意义同上例，则可定义表示，

$$\Gamma^{(2)}(a)=\begin{pmatrix}\lambda & 0\\ 0 & 1/\lambda\end{pmatrix},\Gamma^{(2)}(b)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\Gamma^{(2)}(E)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

由于 p 值在范围 $0\leqslant p\leqslant\frac{n-1}{2}$ 内的表示与在范围 $\frac{n+1}{2}\leqslant p\leqslant n$ 内的表示等价，我们得到 $[(n-1)/2]$ 个不等价的二维表示.

群的表示可以分为不同的等价类. 首先我们将等价表示中结构最简单、便于讨论的表示找出来.

4. 可约表示

从线性变换的观点看，若表示空间 L_n 中存在于空间 $L_m(m\leqslant n)$，在群 G 的作用下是封闭的，即 $\forall\ x\in L_m,\forall\ g_a\in G$，有 $x'=g_a\in L_m$，则 L_m 称为 L_n 的不变子空间.

在线性代数中已经证明，通过适当的线性变换(相似变换)，表示矩阵总可以变为如下三角形式(下三角)：

$$\Gamma(g_a)=\begin{bmatrix}D^{(1)}(g_a) & 0\\ X(g_a) & D^{(2)}(g_a)\end{bmatrix}$$

则该表示 $\{\Gamma(g_a)\}$ 称为可约的. 容易证明 $\{D^{(1)}(g_a)\}$ 与 $\{D^{(2)}(g_a)\}$ 分别为群 G 的 $(n-m)$ 维和 m 维表示.

设 $g_a,g_\beta\in G$，且 $g_ag_\beta=g_\gamma\in G$，则有

$$\Gamma(g_\gamma)=\Gamma(g_ag_\beta)=\Gamma(g_a)\Gamma(g_\beta)=\begin{bmatrix}D^{(1)}(g_\gamma) & 0\\ x(g) & D^{(2)}(g_\gamma)\end{bmatrix}$$

其中

$$D^{(1)}(g_\gamma)=D^{(1)}(g_a)D^{(1)}(g_\beta),$$
$$D^{(2)}(g_\gamma)=D^{(2)}(g_a)D^{(2)}(g_\beta),$$
$$X(g_\gamma)=X(g_a)D^{(1)}(g_\beta)+D^{(2)}(g_a)X(g_\beta).$$

若令 $\forall\ x\in L_n,\forall\ g_a\in G$，

$$\begin{bmatrix}D^{(1)}(g_a) & 0\\ X(g_a) & D^{(2)}(g_a)\end{bmatrix}\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}=\begin{bmatrix}D^{(1)}(g_a) & x\\ X(g_a)x_1+D^{(2)}(g) & x_2\end{bmatrix}$$

可见 x_1(有 $n-m$ 分量)所在的空间 $L_1(n-m$ 维)是不变子空间，即，表示空间存在真子空间(除空间本身外的子空间)与相应表示的可约性互为充要条件.

对于许多群，至少是对有限群，形如三角形的可约表示矩阵可以通过等价变换最后变为对角方块形矩阵，即对 $\forall\ g_a\in G$，有

$$\Gamma(g_\alpha)\to\Gamma'(g_\alpha)=X^{-1}\Gamma(g_\alpha)X\quad(\det X\neq 0)$$

则此表示称为完全可约的. 此时矩阵 $\Gamma^{(a)}(g_\alpha),\Gamma^{(b)}(g_\alpha),\cdots,\Gamma^{(c)}(g_\alpha)$所在的空间 L_a(m_a维),L_b(m_b 维),$\cdots L_c$(m_c 维)均为不变子空间,且

$$m_a+m_b+\cdots+m_c=n,$$

其中 $x_a,x_b,\cdots,x_c$ 分别为矢量 x 的分量,它们分别为 $m_a,m_b,\cdots,m_c$ 维. 也就是说,

$$L_a\oplus L_b\oplus\cdots\oplus L_c=L_n,$$

表示空间可表为它们的直和. 或表示矩阵 $\Gamma(g_\alpha)$可以表示为如下直和形式:

$$(\forall\ g_\alpha\in G):\Gamma(g_\alpha)=\Gamma^{(a)}(g_\alpha)\oplus\Gamma^{(b)}(g_\alpha)\oplus\cdots\oplus\Gamma^{(c)}(g_\alpha).$$

其中$\{\Gamma^{(a)}(g_\alpha)\},\{\Gamma^{(b)}(g_\alpha)\},\cdots,\{\Gamma^{(c)}(g_\alpha)\}$均为群 G 的表示.

若$\{\Gamma^{(a)}(g_\alpha)\}$等都不能再约化,则称此 $\Gamma(g_\alpha)$为"已完全约化的"或"已约表示",而$\{\Gamma^{(a)}(g_\alpha)\}$等不可约表示. 群表示论的中心任务就是要找到群的全部不等价不可约表示,这些表示的相应子空间都是不变子空间. 设集合

$$W=\{L_a,L_b,\cdots L_c\},\forall\ L_i\in W,\forall\ g_\alpha\in G,\text{有 } g_\alpha L_i\subset L_i.$$

5. 表示的幺正性

定理 3.5.1　有限群的每一个等价表示类中,都有一个幺正表示.

证明　设 $\Gamma(g_\alpha)$为群 G 的一个表示,构造以下矩阵,

$$W\equiv\sum_{g_\alpha\in G}\Gamma^+(g_\alpha)\Gamma(g_\alpha)$$

可直接验证矩阵 W 是厄米矩阵:$W^+=W$.

此外,对于给定 $\Gamma(g_\beta)$,

$$\begin{aligned}\Gamma^+(g_\beta)W\Gamma(g_\beta)&=\sum_{g_\alpha\in G}\Gamma^+(g_\beta)\Gamma^+(g_\alpha)\Gamma(g_\alpha)\Gamma(g_\beta)\\&=\sum_{g_\alpha\in G}(\Gamma(g_\alpha)\Gamma(g_\beta))^+(\Gamma(g_\alpha)\Gamma(g_\beta))\\&=\sum_{g_\alpha\in G}\Gamma^+(g_\alpha g_\beta)\Gamma(g_\alpha g_\beta)\\&=W,\end{aligned}$$

即 $\Gamma^+(g_\beta)W\Gamma(g_\beta)=W$. 由于 W 的厄米性,故可将 W 表为 $W=X^+X$(X 为 $n\times n$ 正则矩阵). 其 X 矩阵即为将表示$\{\Gamma(g_\alpha)\}$变为幺正矩阵$\{\Gamma'(g_\alpha)\}$的变换矩阵,即

$$\Gamma'(g_\alpha)=X\Gamma(g_\alpha)X^{-1}.$$

事实上,对任意 $g_\alpha\in G$,应有

$$\begin{aligned}\Gamma'^+(g_\alpha)\Gamma'(g_\alpha)&=(X\Gamma^+(g_\alpha)X^{-1})^+(X\Gamma(g_\alpha)X^{-1})\\&=(X^{-1})^+\Gamma^+(g_\alpha)X^+X\Gamma(g_\alpha)X^{-1}\end{aligned}$$

$$=(X^{+})^{-1}\Gamma^{+}(g_{\alpha})W\Gamma(g_{\alpha})X^{-1}$$
$$=(X^{+})^{-1}WX^{-1}=(X^{+})^{-1}X^{+}XX^{-1}$$
$$=E\ (n\times n\ \text{单位矩阵}).$$

本定理可以进一步推广为：联系两个等价的幺正表示的相似变换，总可以是幺正的.

定理的另一个推广是，它的实用范围可由有限群推广到紧致连续群. 注意定理证明的关键是构造厄米矩阵 W. 对于有限群，求和项数有限，W 必然存在. 推广到连续群后，$\sum_{g_\alpha\in G}$ 换成对群参数积分

$$\int\Gamma^{+}(g_{\alpha})\Gamma(g_{\alpha})\mathrm{d}\alpha.$$

如果积分收敛，则 W 亦存在. 对于紧致群，群参数只在参数空间有限范围内取值，积分收敛，故定理亦成立. 至于非紧致群，如洛仑兹群定理也成立. 但一般情况下，对于非紧致群本定理不成立.

等价性的引入，使得寻求群的全部表示的问题简化为寻求群的全部不等价的表示，可约性的引入，使得问题进一步简化为寻求群的全部不等价、不可约的表示；玛克(Machke)定理更将问题简化为寻求群的全部不等价、不可约的幺正表示.

舒尔引理是判断群的一个表示是否可约的理论基础，在群表示理论中占极其重要的地位. 在此针对有限群的情况加以证明，其适用范围可推广到连续紧致群.

Schur 引理一　设 $\{\Gamma(g_\alpha)\}$ 为群 G 的不可约表示，其维数为 l，M 为 $l\times l$ 矩阵($\det M\neq 0$)，且对任意 $g_\alpha\in G$，有 $M\Gamma(g_\alpha)=\Gamma(g_\alpha)M$，则 $M=\lambda E$(E 是单位矩阵).

证明　设 x_0 为 M 的一个本征矢，即 $Mx_0=\lambda x_0$，$x_0\in L_l$，令 $x_0^\alpha\equiv\Gamma(g_\alpha)x_0$ 亦为 M 的本征矢，本征值亦为 λ，事实上，

$$Mx_0^\alpha=M\Gamma(g_\alpha)x_0=\Gamma(g_\alpha)Mx_0=\lambda\Gamma(g_\alpha)x_0=\lambda x_0^\alpha$$

则矢量 $\{x_0^\alpha\,|\,x_0^\alpha=\Gamma(g_\alpha)x_0,\forall\ g_\alpha\}$ 张成子空间 L_0. 对 $\forall\ g_\alpha,g_\beta\in G$，有

$$\Gamma(g_\beta)x_0^\alpha=\Gamma(g_\beta)\Gamma(g_\alpha)x_0=\Gamma(g_\alpha g_\beta)x_0$$
$$=\Gamma(g_\gamma)x_0=x_0^\gamma\in L_0(g_\alpha g_\beta=g_\gamma\in G),$$

即在任何群元作用下，L_0 是封闭的，也就是不变子空间.

但已知 $\{\Gamma(g_\alpha)\}$ 为不可约表示，因而不应有真不变子空间. 这意味着只会存在下述两种情况.

(1)$L_0=\varnothing$(空集). 由于在复空间中任何正则矩阵至少有一本征矢，这种情况应予否定. 这样，唯一可能的情况是(2).

(2)$L_0=L$，$\forall\ x\in L$，即所有属于 L 空间矢量 x 均是 M 的本征矢，本征值为 λ，即 M

$=\lambda E$.

Schur 引理一的逆命题亦成立. 由下面例子可以推知的确如此.

例 3.5.6　可约表示 $\Gamma(g_a)$一定可以化为直和形式,$D^{(1)}(g_a)$为 l_1 维,$D^{(2)}(g_a)$为 l_2 维.

$$X^{-1}\Gamma(g_a)X=\begin{bmatrix} D^{(1)}(g_a) & O \\ O & D^{(2)}(g_a)\end{bmatrix}$$

此矩阵显然可与非常数矩阵

$$M'=\begin{bmatrix} \lambda_1 I_1 & O \\ O & \lambda_2 I_2\end{bmatrix}(\lambda_1\neq\lambda_2, I_1、I_2 \text{ 为 } l_1 \text{ 维与 } l_2 \text{ 维单位矩阵})$$

对易. 这就是舒尔引理一的逆命题.

Schur 引理二　设$\{\Gamma^{(a)}(g_a)\}$与$\{\Gamma^{(b)}(g_\beta)\}$为群 G 的两个不等价不可约表示,维数分别为l_a与l_b,若存在 $l_a\times l_b$ 矩阵 M,对于$\forall\ g_a\in G$,有 $M\Gamma^{(a)}(g_a)=\Gamma^{(b)}(g_\beta)M$,则 $M=O$(零阵).

证明　表示$\{\Gamma^{(a)}(g_a)\}$与$\{\Gamma^{(b)}(g_a)\}$都可以通过相似变换化为幺正表示,而零矩阵不因相似变换而改变,故只需证明$\{\Gamma^{(a)}(g_a)\}$与$\{\Gamma^{(b)}(g_a)\}$为幺正表示成立就可以了. 这并不失一般性.

在上式两端取厄米共轭,并注意到

$$\Gamma^{(a)}(g_a)^+=\Gamma^{(a)}(g_a),\Gamma^{(b)}(g_a)^+=\Gamma^{(b)}(g_a),$$

得

$$\Gamma^{(a)}(g_a)M^+=M^+\Gamma^{(b)}(g_a)$$

用 M 左乘此式,并利用题设条件,有

$$M\Gamma^{(a)}(g_a)M^+=MM^+\Gamma^{(b)}(g_a)=\Gamma^{(b)}(g_a)MM^+.$$

由 Schur 引理一,$MM^+=\lambda E_2$(E_2 为 l_b 维单位矩阵). 若 $l_a=l_b$,则题设条件变为

$$\Gamma^{(b)}(g_a)=M\Gamma^{(a)}(g_a)M^{-1}.$$

但已知$\{\Gamma^{(a)}(g_a)\}$与$\{\Gamma^{(b)}(g_a)\}$是不等价的,故 M 必为 $\det M=0$ 的非正则矩阵. 但 $MM^+=\lambda E_2(l_a\times l_b)$,因此

$$\det M\cdot\det M^+=(\lambda)^{l_b}=0\Rightarrow\lambda=0.$$

另一方面,$MM^+=\lambda E_2(l_a\times l_b)$,即

$$\lambda=\sum M_{\mu\nu}M_{\mu\nu}^*=\sum_{\mu,\nu=1}^{l_b}|M_{\mu\nu}|^2=0,$$

即 $M_{\mu\nu}=0(\mu,\nu=1,2,\cdots,l_b)$. 若 $l_a\neq l_b$,为确定起见,令 $l_a<l_b$. 将 M 阵添加(l_a-l_b)行零,则 M 变成 $l_a\times l_b$ 的方阵 N,由矩阵乘法可知 $NN^+=MM^+$. 代入上式,得 $NN^+=\lambda E_2$. 此时完全等同于 $l_a=l_b$ 的情况,故知 N 为零矩阵,即 M 为零矩阵. 由此第二引理得证.

问题 3.5

1. 验证二面体集合 D_n 构成一个群，以及有关系式：

$$aba=b, ab=ba^{n-1}, ba=a^{n-1}b.$$

2. 试证 $\forall\ x,y\in L_n$，$y=\Gamma(g_a)x$，当进行基底变换：$b'=X^{-1}b$ 时（X 为 $n\times n$ 正则矩阵），有 $x'=Xx$，$y'=Xy$，$\Gamma'(g_a)=X\Gamma(g_a)=X^{-1}$，$y'=\Gamma'(g_a)x'$.

3. 证明有限群 G 的两个等价幺正表示 $\{\Gamma(g)\}$ 与 $\{\Gamma'(g)\}$ 总可以通过相似的幺正变换联系起来.

4. 证明有限群幺正表示或者是不可约的，或者是完全可约的（只需证明幺正表示如可约，则必完全可约）.

5. 证明下三角矩阵 $A=\{A_{ij}\}$（其中 $A_{ij}=0$，当 $j>i$）的乘积依然是下三角矩阵；若 $\det A\neq 0$，下三角矩阵的逆亦为下三角矩阵；若 $\forall\ A_{ij}\in\Omega(c)$，则下三角矩阵的集合形成群.

6. 设 M 为 $n\times n$ 的正则矩阵，若 $\forall\ x\in L_n$ 均为其本征值相同(λ)的本征矢，即 $Mx=\lambda x$，则 M 必为 λE（E 为 $n\times n$ 单位矩阵）.

7. 若 $\{\Gamma^{(a)}(g_a)\}$ 与 $\{\Gamma^{(b)}(g_a)\}$ 为非幺正表示，影响 Schur 引理二的证明吗？试论述之.

§3.6　群的特征标

本节介绍群的表示以及特征标的基本性质，我们会看到代数的表示与群的表示的密切联系. 设 V 是域 F 上的 n 维向量空间，$GL(V)$ 表示 V 的全体可逆线性变换关于变换的乘法组成的群，$GL_n(F)$ 表示 F 上全体 $n\times n$ 矩阵关于矩阵的乘法组成的群，当然两者是同构的. 与代数的表示概念类似，我们有下列群表示的定义.

定义 3.6.1　群 G 到 $GL(V)$ 的一个同态映射 φ 称为 G 的一个（线性）表示，而群 G 到 $GL_n(F)$ 的一个同态映射 φ 称为 G 的一个（矩阵）表示. V 称为表示空间，而 $\dim_F V=n$，矩阵的级称为表示的级.

基于与代数的表示同样的理由，以后我们谈群的表示时，不再区分是矩阵表示还是线性表示，而视讨论问题的需要采取所需形式.

和代数的表示一样，我们同样可定义群的两个表示等价的概念，在此不再叙述. 下面将会看到，等价的表示可看作是相同的.

在定理 3.1.4 我们看到，群 G 到 $GL(V)$ 的一个表示可定义一个 FG 模 V，由上节的讨论又知，一个 FG 模 V 可定义群代数 FG 到 $\mathrm{End}_F(V)$ 的一个表示. 反之，给定群代

数 FG 到 $\mathrm{End}_F(V)$ 的一个表示，其在 G 上的限制得到 G 的一个表示，因而研究群的表示与研究群代数的表示是一回事. 代数的表示可通过代数上的模来研究，因而群的表示可通过群代数上的模来研究，与代数的表示一样，我们可定义群的不可约表示、忠实表示以及正则表示等差别在于把代数换成群代数来叙述.

根据以上分析，群表示论的基本问题之一也是决定群 G 在域 F 上的所有不等价的不可约表示，而这等价于决定所有互不同构的不可约 FG 模. 由 Maschke 定理知，当域 F 的特征为零或其特征不整除 $|C|$ 时，不可约 FG 模(或单 FG 模)可以完全确定，因而对群 G 的表示的研究可归结为不可约表示的研究. 而当 F 的特征整除 $|C|$ 时，情况就大不相同了，前者称为常表示，后者称为模表示.

设 G 表示有限群，下面考虑的 CG 模是有限生成的，或等价地说，作为 C 向量空间是有限维的，其中 C 是复数域. 因为 C 是特征为零的代数闭域，由半单代数的结构定理我们可得群代数 C 的深刻特征.

定理 3.6.1　(1)若把 CG 看作为 C 代数，则存在 $r\in\mathbf{N}$ 以及 $n_1,\cdots,n_r\in\mathbf{N}$ 使得 $CG\cong M_{n_1}(C)\oplus\cdots\oplus M_{n_r}(C)$；

(2)若把 CG 看作为 CG 模，则恰好有 r 个单 CG 模的同构类. 若令 $S_1,\cdots,S_r$ 构类的代表，则可适当调整次序使得

$$CG\cong n_1S_1\oplus\cdots\oplus n_rS_r,$$

其中对每个 i 来说，$\dim_C S_i=n_i$；

(3)若 M 是一个 CG 模，则 $M=a_1S_1\oplus\cdots\oplus a_rS_r$，其中 a_i 是唯一确定的非负整数.

证明　由定理 3.3.5 及 3.3.8 可得(1)；取 S_i 是由 n_i 维列向量构成的向量空间，依照矩阵乘法，S_i 作成 $M_{n_i}(C)$模，由定理 3.3.6 及 3.3.10 可得(2)；由定理 3.3.5 可得(3).

这 r 个单 CG 模的维数 $n_1,\cdots,n_r$ 称为 G 的次数. 平凡 CG 模 C 是一维的，因而是单模，故 C 的次数中至少有一个等于 1. 按照惯例，我们记 $n_1=1$.

定理 3.6.2　n_i 如定理 3.6.1 所设，则 $\sum_{i=1}^{r}n_i^2=|G|$.

证明　由定理 3.6.1 可得，

$$|G|=\dim_C CG=\dim_C(\bigoplus_{i=1}^{r}M_{n_i}(C))=\sum_{i=1}^{r}\dim_C M_{n_i}(C)=\sum_{i=1}^{r}n_i^2.$$

下面我们给出单 CG 模的个数与群 G 的结构之间的一个联系.

定理 3.6.3　单 CG 模的个数等于群 G 的共轭类的个数.

证明　设 Z 是 CG 的中心，由定理 3.6.1 易知，Z 同构于 $M_{n_1}(C)\oplus\cdots\oplus M_{n_r}(C)$ 的中心，因而同构于每个 $M_{n_i}(C)$ 中心的直和. $M_{n_i}(C)$ 中心由数量矩阵组成，从而它与 C 同

构，于是 $Z \cong C^r$. 特别地，$\dim_C Z = r$.

设 $\sum_{g\in G} k_g g \in \mathbf{Z}$，对任意的 $h \in C$，我们有

$$\left(\sum_{g\in G} k_g g\right)h = h\left(\sum_{g\in G} k_g g\right).$$

由此得

$$\sum_{g\in G} k_g g = \sum_{g\in G} k_g h^{-1} gh = \sum_{g\in G} k_{hgh^{-1}} g,$$

因而对任意的 $g, h \in G$，我们有 $k_g = k_{hgh^{-1}}$.

这就是说，Z 中元素的系数在 G 的共轭类上是常数，因而 Z 的一个基是由形如 $\sum_{g\in G} g$ 的这样一些元素构成，其中 K 是 G 的一个共轭类，于是 $\dim_C Z$ 等于群 G 的共轭类的个数.

特征标理论最初是由 Frobenius 和其他人于 1896 年提出的. 这里介绍的特征标的概念就是以迹函数的语言来定义的.

定义 3.6.2　设 U 是一个 CG 模，对每个 $g \in G$，由 g 我们可定义 U 的一个可逆线性变换 $u \longmapsto gu$，我们定义 U 的特征标是一个函数 $\chi_U : G \to C$，其中 $\chi_U(g)$ 是由 g 定义的 U 的可逆线性变换的迹.

例如，$\chi_U(1) = \dim_C U$，如果 $\rho: G \longrightarrow GL(U)$ 是 G 在 U 上的线性表示，则 $\chi_U(g)$ 恰好等于 $\rho(g)$ 的迹.

群 C 的任何两个共轭元的特征标的值是相同的. 这是因为对任意的 $g, h \in G$，由 g 和 $h^{-1}gh$ 定义的 U 的线性变换是相似的，因而有相同的迹. 另外，由定理 3.4.1 又知，同构的 CG 模有相等的特征标.

设 $U = CG$，$g \in G$，考虑 g 在 CG 的基 G 上定义的线性变换的矩阵，则 $\chi_U(g)$ 恰好等于 G 中满足 $gx = x$ 的元素 x 的个数，于是，当 $g = 1$ 时，$\chi_U(g) = |G|$；而当 $g \neq 1$ 时，$\chi_U(g) = 0$，这个特征标称为 G 的正则特征标.

定义 3.6.3　用 $\chi_1, \cdots, \chi_r$ 表示定理 3.5.1 中的 r 个单 CG 模的特征标，这些特征标称为 G 的不可约特征标，记为 $\mathrm{Irr}(G) = \{\chi_1, \cdots, \chi_r\}$.

以后只要我们说 $S_1, \cdots, S_r$ 是不同的单 CG 模，则我们总可以调整次序使得对每个 i 来说，记 $\chi_{S_i} = \chi_i$. 另外，用 n_1 表示平凡表示的次数，χ_1 表示平凡表示的特征标，并称 χ_1 为 G 的主特征标.

显然，对所有的 $g \in G$ 来说，$\chi_1(g) = 1$. 有时也记 $\chi_1 = 1_G$.

一维 CG 模的特征标称为线性特征标，因为一维 CG 模一定是单模，故线性特征标必是不可约的. 线性特征标等价于群 G 到复数乘群 C^* 的一个同态，这是因为，若 χ 是一维 CG 模 U 的一个线性特征标，则对于 $g, h \in G$，$u \in U$，我们有 $gu = \chi(g)u$，$hu =$

$\chi(h)u$，于是 $\chi_1(gh)u=(gh)u=\chi(g)\chi(h)u$，故 χ 是 G 到 C^* 的一个同态；反之，给定一个同态 $\varphi:G\longrightarrow C^*$，对于 $g\in G,u\in U$，令 $gu=\varphi(g)u$，则我们定义了一个一维 CG 模 U，并且有 $\chi_U=\varphi$.

关于特征标，我们给出下列基本结果.

定理 3.6.4　设 U 是 CG 模，$\rho:G\to GL(U)$ 是 G 在 U 上的表示，$g\in G$，其阶为 n，则：

(1) $\rho(g)$ 可对角化；

(2) $\chi_U(g)$ 等于 $\rho(g)$ 的特征值的和；

(3) $\chi_U(g)$ 等于 $\chi_U(1)$ 个 n 次单位根的和；

(4) $\chi_U(g^{-1})=\overline{\chi_U(g)}$（这里 $\bar{z}$ 表示复数 z 的复共轭）；

(5) $|\chi_U(g)|\leqslant\chi_U(1)$；

(6) $\{x\in G\mid\chi_U(x)=\chi_U(1)\}\lhd G$.

证明　(1) 因为 $g^n=1$，$\rho(g)$ 满足多项式 x^n-1，但 x^n-1 在复数域上可分解成一次因式的乘积，故 $\rho(g)$ 的极小多项式也能分解成一次因式的乘积，因而 $\rho(g)$ 可对角化；

(2) $\rho(g)$ 的迹是它的特征值的和，即 $\chi_U(g)$ 等于 $\rho(g)$ 的特征值的和；

(3) 因为 $\rho(g)$ 的特征根恰好是它的极小多项式的根，而 $\rho(g)$ 的极小多项式整除 x^n-1，故这些根都是单位根，又 $\chi_U(1)=\dim_C U$，所以 $\chi_U(g)$ 等于 $\chi_U(1)$ 个 n 次单位根的和；

(4) 由高等代数知，$\rho(g)$ 的特征向量也是 $\rho(g^{-1})$ 的特征向量，$\rho(g^{-1})$ 的特征值是 $\rho(g)$ 特征值的逆，因为 $\rho(g)$ 特征值是单位根，故 $\rho(g^{-1})$ 的特征值是 $\rho(g)$) 特征值的共轭，由此得(4) 成立；

(5) 由(3) 直接可得；

(6) 由上述证明看 $\chi_U(g)$ 是 $\chi_U(1)$ 个特征值的和，且这些特征值均为单位根. 如果 $\rho(g)=\chi_U(1)$，则这些特征值必均等于 1，于是 $\rho(g)$ 一定是恒等映射. 反之，若 $\rho(g)$ 是恒等映射，则必有 $\chi_U(g)=\dim_C(U)=\chi_U(1)$，由此得

$$\{x\in G\mid\chi_U(x)=\chi_U(1)\}=\mathrm{Ker}\rho\lhd G.$$

给定 $k\in G$，我们定义由 G 到 C 的一个新函数 k_χ，其中 $(k_\chi)(g)=k_\chi(g)$，$g\in G$. 于是 G 的特征标可看为由 G 到 C 的函数构成的复数域 C 上的向量空间中的元素.

定理 3.6.5　若把 G 的特征标看作为由 G 到 C 的函数，则 G 的不可约特征标在 C 上是线性无关的.

证明　由定理 3.6.1 知，$CG\cong M_{n_1}(C)\oplus\cdots\oplus M_{n_r}(C)$，令 $S_1,\cdots,S_r$ 是不同构的单 CG 模，对每个 i，令 e_i 是 $M_{n_i}(C)$ 的单位矩阵. 固定某个 i，我们知道，对任意的 $g\in G$，

$\chi_i(g)$ 是由 g 定义的 S_i 上的一个线性变换的迹. 现在我们把 χ_i 线性扩张为 CG 到 C 的一个线性映射,使得对任意的 $a \in CG$, $\chi_i(a)$ 是由 a 定义的 S_i 上的一个线性变换的迹. 容易看出,由 e_i 定义的 S_i 上的一个线性变换是恒等变换,因而 $\chi_i(e_i) = \dim_C S_i$,若 $j \neq i$,则由 e_i 定义的 S_j 上的一个线性变换是零变换,因而 $\chi_i(e_i) = 0$. 设 $k_1, \cdots, k_r \in C$,并且 $\sum_{j=1}^{r} k_j\chi_j = 0$,对每个 i 来说,$0 = \sum_{j=1}^{r} k_j\chi_j(e_j) = k_i n_i$,于是对所有的 i 来说,$k_i = 0$. 结论得证.

引理 3.6.6 对任意 CG 模 U 和 V 来说,$\chi_{U\oplus V} = \chi_U + \chi_V$.

证明 把 U 的一个基与 V 的一个基放在一起构成 $U \oplus V$ 的一个基,则对任意的 $g \in G$ 我们有 $\chi_{U\oplus V}(g) = \chi_U(g) + \chi_V(g)$,结论得证.

由引理 3.6.6 的证明可知,若 χ 和 ψ 是 G 的特征标,则我们可定义由 G 到 C 的新函数 $\chi + \psi$,其中 $(\chi + \psi)(g) = \chi(g) + \psi(g)$, $g \in G$,则 $\chi + \psi$ 也是 G 的特征标.

下面我们利用特征标给出判断两个 CG 模是否同构的一个准则.

定理 3.6.7 如果 $S_1, \cdots, S_r$ 是不同的单 CG 模,则 CG 模 $a_1S_1 \oplus \cdots \oplus a_rS_r$ 的特征标是 $a_1\chi_1 + \cdots + a_r\chi_r$,其中 a_i 是非负整数. 因而两个 CG 模同构当且仅当它们的特征标是相等的.

证明 由引理 3.6.6 可得定理的第一个结论,设对于 CG 模 U 和 V 来说,$\chi_U = \chi_V$,因为 CG 模均为半单的,不妨设 $U \cong \oplus_i a_iS_i$, $V \cong \oplus_i b_iS_i$,其中 a_i 和 b_i 是非负整数. 计算特征标得 $0 = \chi_U - \chi_V = \Sigma_i(a_i - b_i)\chi_i$,由定理 3.6.5 得,对 $\forall\, i, a_i = b_i$,因而 $U \cong V$.

在同构的意义下,一个特征标可唯一确定一个 CG 模,但已知某个模的特征标,我们还没有一个一般的方法来构造这个模. 利用特征研究模,目前结果甚少,然而以后我们会看到,特征标能有效地从群 G 的常表示的有关信息得到 G 本身的信息,因此下面我们把注意力从 CG 模转向它们的特征标.

由前几节我们知道,若 U 和 V 是 CG 模,则 $U \odot_C V$ 和 $\mathrm{Hom}_C(U, V)$ 也是 CG 模. 下面我们考虑这两个 CG 模与 U 和 V 之间的关系.

定理 3.6.8 设 U 和 V 是 CG 模,则:

(1) $\chi_{U\oplus V} = \chi_U\chi_V$;

(2) $\chi_{U^*} = \overline{\chi_U}$,其中 $U^* = \mathrm{Home}(U, V)$;

(3) $\chi_{\mathrm{Hom}(U,V)} = \overline{\chi_U}\chi_V$.

证明 (1) 设 $g \in G$,由定理 3.6.4(1) 知,g 在 U 上定义的线性变换是可对角化的,令 $\{u_1, \cdots, u_m\}$ 是 U 的特征向量构成的一个基,其对应的特征值分别是 $\xi_1 \cdots, \xi_m$;类似地,令 $\{v_1, \cdots, v_n\}$ 是 g 在 V 上定义的线性变换的特征向量构成的一个基,其对应的特征值分别是 $\eta_1, \cdots, \eta_n$,于是由定理 3.6.4 (2) 我们有

$$\chi_U(g)=\xi_1+\cdots+\xi_m,\chi_V(g)=\eta_1+\cdots+\eta_m,$$

又$\{u_i\odot v_j\}_{i,j}$是$U\odot V$的一个基,并且对任意的i,j来说,

$$g(u_i\odot v_j)=gu_i\odot gv_j=\xi_iu_i\odot\eta_jv_j=\xi_i\eta_j(u_i\odot v_j),$$

于是,$\{u_i\odot v_j\}_{i,j}$是g在$U\odot V$上定义的线性变换的特征向量构成的一个基,由此得

$$\chi_{U\oplus V}(g)=\sum_{i,j}\xi_i\eta_j=(\sum_i\xi_i)(\sum_j\eta_j)=\chi_U(g)\chi_V(g).$$

(2) 设$g\in G$,仍令$\{u_1,\cdots,u_m\}$是g在U上定义的线性变换的特征向量构成的一个基,其对应的特征值分别是$\xi_1\cdots,\xi_m$,令$(\varphi_1,\cdots,\varphi_m)$是$U^*$的对偶基,其中$\varphi_i:U\to C$如下定义:对每个$i,j,\varphi_i(u_j)=a_{ij}$,固定某个$j$,则$gu_j=\xi_j^{-1}u_j$,又由定理3.6.4的证明知,$\xi_j$是单位根,因而有$\xi_j^{-1}=\overline{\xi_j}$,于是对于$\forall\ i,j$,有

$$g(\varphi_i)(u_j)=\varphi_i(g^{-1}u_j)=\varphi_i(\overline{\xi_j}u_j)=\overline{\xi_j}a_{ij}$$

由此得出对每个i均有$g\varphi_i=\overline{\xi_j}\varphi_i$,这说明,$(\varphi_1,\cdots,\varphi_m)$是$U^*$的由$g$定义的线性变换的特征向量构成的一个基,其对应的特征值分别是$\overline{\xi_1},\cdots,\overline{\xi_m}$,因而

$$\chi_{U^*}(g)=\overline{\xi_1}+\cdots+\overline{\xi_m}=\overline{\xi_1+\cdots+\xi_m}=\overline{\chi_U(g)}.$$

(3) 又有$\mathrm{Home}(U,V)\cong U^*\odot V$.因而(3)可由(1)和(2)得到.

我们把G的不可约特征标的Z线性组合称为G的广义特征标.由定理3.6.7知特征标都是广义特征标.

定理 3.6.9 G的广义特征标构成一个环.

证明 由定理3.6.1(1)知,两个特征标的乘积还是一个特征标,其余的可由定义直接验证.

如果G到C的一个函数在G的共轭类上取值相同,则这个函数称为G的一个类函数,于是CG模的特征标是一个类函数,G上所有类函数的集合构成一个复数域C上的r维向量空间,其中r是G的共轭类的个数,把这个向量空间记为$cf(G)$.若令φ是G上的类函数,它在由单个元素构成的共轭类上取值为1,而在其他共轭类上取值为零,则所有这样的类函数构成这个向量空间的一个基,除此之外,我们还可找到这个向量空间的其他基.

定理 3.6.10 G的不可约特征标是G上类函数构成的向量空间$cf(G)$的一个基.

证明 由定理3.6.5知,G的不可约特征标在G的类函数构成的向量空间上是线性无关的,又由定理3.6.3知,G的不可约特征标的个数等于G的共轭类的个数,而G的共轭类的个数又等于G上类函数构成的向量空间的维数,由此得证.

设α,β是G的两个类函数,定义它们的内积为

$$(\alpha,\beta)=\frac{1}{|G|}\sum_{g\in G}\alpha(g)\overline{\beta(g)},$$

这个函数具有下列性质：

1) $\forall\ \alpha,(\alpha,\alpha)\geqslant 0$，且$(\alpha,\alpha)=0$当且仅当$\alpha=0$；

2) 对$\forall\ \alpha,\beta,(\alpha,\beta)=\overline{(\beta,\alpha)}$；

3) 对$\forall\ \alpha,\beta$以及$k\in C,(k\alpha,\beta)=k(\alpha,\beta)$；

4) 对$\forall\ \alpha_1,\alpha_2,\beta(\alpha_1+\alpha_2,\beta_2)=(\alpha_1,\beta)+(\alpha_2,\beta)$.

5) 对$\forall\ \alpha,\beta$以及$k\in C,(\alpha,k\beta)=\bar{k}(\alpha,\beta)$；

6) 对$\forall\ \alpha,\beta_1,\beta_2,(\alpha,\beta_1+\beta_2)=(\alpha,\beta_1)+(\alpha,\beta_2)$.

最后给出两个特征标的内积的一个刻画，为此先介绍有关概念及引理.

如果U是一个CG模，令$U^G=\{u\in U\ |\forall\ g\in G,gu=u\}$，则$U^G$是$U$的子模.

定理 3.6.11　若U是一个CG模，则$\dim_C U^G=\dfrac{1}{|G|}\sum\limits_{g\in G}\chi_U(g)$.

证明　设$a=\dfrac{1}{|G|}\sum\limits_{g\in G}g\in CG$，则对$\forall\ g\in G,ga=a$，由此可见$a^2=a$，设$T$是由$a$定义的$U$上的线性变换，则$T$满足方程$x^2-x=0$，因而$T$可对角化，且$T$的特征值只能是0或1.令$U_1$是与特征值1相对应的$T$的特征子空间，若$u\in U_1$，则对$\forall\ g\in G$，$gu=gau=au=u$，因而$u\in U^G$.

反之，设$u\in U^G$，则我们有

$$|G|au=(\sum_{g\in G}g)u=\sum_{g\in G}gu=\sum_{g\in G}u=|G|u,$$

因而$au=u$，这就得到，$u\in U_1$，故$U^G=U_1$.又T的迹等于U_1的维数，由迹映射的线性性，结论得证.

定理 3.6.12　对任意的CG模U和V来说，$(\chi_U,\chi_V)=\dim_C\mathrm{Hom}_{CG}(U,V)$.

证明　首先我们注意到$\mathrm{Hom}_{CG}(U,V)$是CG模$\mathrm{Hom}_C(U,V)$的子空间，若$\varphi\in\mathrm{Hom}_{CG}(U,V)$且$g\in G$，则$(g\varphi)(u)=g\varphi(g^{-1}u)=gg^{-1}\varphi(u)=\varphi(u)$，因而对$\forall\ g\in G$，$g\varphi=\varphi$.这就证明了$\varphi\in\mathrm{Hom}_C(U,V)^G$.

反过来，这包含关系也成立，因而$\mathrm{Hom}_{CG}(U,V)=\mathrm{Hom}_C(U,V)^G$，于是由定理3.6.4和定理3.6.1(3)，我们有

$$\begin{aligned}\dim_C\mathrm{Hom}_{CG}(U,V)&=\dim_C\mathrm{Hom}_C(U,V)^G\\&=\frac{1}{|G|}\sum_{g\in G}\chi_{\mathrm{Hom}_C(U,V)}(g)=\frac{1}{|G|}\sum_{g\in G}\overline{\chi_U(g)}\chi_V(g)=(\chi_V,\chi_U)\end{aligned}$$

因为(χ_V,χ_U)是实数，$(\chi_U,\chi_V)=\dim_C\mathrm{Hom}_{CG}(U,V)$.

下面我们继续研究特征标的基本性质.

行正交定理　对$\forall\ i,j$来说，$(\chi_i,\chi_j)=a_{ij}$.

证明　设$S_1,\cdots,S_r$是不同的单CG模，由定理3.6.5知，对$\forall\ i,j,(\chi_i,\chi_j)=$

$\dim_C \mathrm{Hom}_{CG}(S_i, S_j)$. 对 $\forall\ i$, $\mathrm{Hom}_{CG}(S_i, S_j) = \mathrm{End}_{CG}(S_i, S_j) \cong C$. 又由 Schur 引理，当 $i \neq j$ 时，$\mathrm{Hom}_{CG}(S_i, S_j) = 0$.

上述定理告诉我们对 $\forall\ i$ 和 j，

$$\delta_{ij} = \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\,\overline{\chi_j(g)} = \frac{1}{|G|}\sum_{t=1}^{r}k_t\chi_i(g_t)\,\overline{\chi_j(g_t)}$$

其中，g_t 是 G 的共轭类的代表元，k_t 是 G 的含 g_t 的共轭类的元素个数，当我们把特征标的行看为 C^r 的向量时，我们可以说特征标表的任意两行关于内积是正交的，这就是行正交定理名称的来源. 由行正交定理，我们可得出许多重要的结果.

推论 3.6.13　G 的不可约特征标是 G 的类函数构成的向量空间 $cf(G)$ 的一个正交基.

推论 3.6.14　设 $\alpha = \Sigma_i a_i\chi_i$ 和 $\beta = \Sigma_j b_j\chi_j$ 是 G 的广义特征标，则 $(\alpha, \beta) = \Sigma_i a_i b_i$.

定理 3.6.15　设 α 是 G 的特征标，$n \in \{1, 2, 3\}$，则 $(\alpha, \alpha) = n$ 当且仅当 α 是 n 个不可约特征标的和.

证明　设 $\alpha = \sum_{i=1}^{r}a_i\chi_i$，其中 a_i 是非负整数，由定理 3.6.2 有 $(\alpha, \alpha) = \Sigma_i a_i^2$，若 $(\alpha, \alpha) = n$，则对于 n 个数而言，当 $1 \leqslant j \leqslant n$ 时，必有 $a_j = 1$，对于其他的 i，$a_i = 0$. 在这种情况下，α 是 n 个不可约特征标的和.

反之，由定理 3.6.2 直接可得.

定理 3.6.16　如果 α 是一个广义特征标，则 α 作为 G 的不可约特征标的 Z 线性组合，其表达式是唯一的，且每个 χ_j 在这个表达式中的系数是 (α, χ_j).

更一般地，若 $0 \neq \psi \in cf(G)$，则 ψ 是 G 的特征标当且仅当对所有的 $\chi \in \mathrm{Irr}(G)$ 都有 (ψ, χ) 是非负整数.

证明　由定义可设 $\alpha = \sum_{i=1}^{r}a_i\chi_i$，其中 a_i 是非负整数，则 $(\alpha, \chi_j) = a_j$.

对于后一个结论，证明如下：若 ψ 是 G 的特征标，由定理 3.6.5 可知结论成立. 反之，由推论 3.6.6 知，$\psi = \Sigma_{\chi\in \mathrm{Irr}(G)}c\chi$，其中 $c \in C$. 由正交性又得 $c = (\psi, \chi)$，由假设得 c 是非负整数，于是 ψ 是一些不可约特征标之和，知 ψ 是 G 的特征标.

问题 3.6

1. $\{\Gamma^{(i)}(g_\alpha)\}$ 与 $\{\Gamma^{(j)}(g_\alpha)\}$ 为群 G 的不可约表示，维数为 l_i 与 l_j，X 为 $l_i \times l_j$ 非零矩阵，若 $M = \sum_{g_\alpha}\Gamma^{(i)}(g_\alpha)X\Gamma^{(j)}(g_\alpha^{-1})$，验证：$\Gamma^{(i)}(g_\beta)M = M\Gamma^{(j)}(g_\alpha)$.

2. 证明群 G 的不可约表示与一维表示的乘积是不可约表示.

3. 若群 G 的表示 $\{\Gamma(g_\alpha)\}$ 的特征标矢量在 L_G 中的内积 $(\chi, \chi) = 1$，证明此表示不

可约.

4. 若$\{\Gamma(g_a)\}$为群的表示,则$\{\Gamma(g_a)\}$与$\{\Gamma^*(g_a)\}$同为可约表示或不可约表示,这里$\{\Gamma^*(g_a)\}$是$\{\Gamma(g_a)\}$的复共轭.

§3.7　群的特征标表

由上节我们知道,G的任何一个特征标是G的r个不可约特征标的Z线性组合,由定理3.6.3知,r等于C的共轭类的个数.因为每一个不可约特征标是由它在G的每一个共轭类上的值完全确定,因而G的特征标完全由G的r个不可约特征标在G的r个共轭类上的值确定.把这$r\times r$个数作成一个表,这个表称为G的特征标表.

显然,如果适当调整这个表的行和列的元素,G的特征标表是唯一确定的.

令Γ表示G的特征标表,则$\Gamma=\chi_i(g_j)1\leqslant i,j\leqslant r$,其中$g_1,\cdots,g_r$是$G$的$r$个共轭类的代表元.不妨令$g_1=1$,特征标表的第一列由$G$的次数组成,一般地,我们把$G$的特征标表$\Gamma$写为以下形式:

	1	k_2	k_r
	1	g_2	g_r
χ	1	1	1
χ	n_2	$\chi_2(g_2)$	$\chi_2(g_2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
χ	n_r	$\chi_r(g_2)$	$\chi_r(g_2)$

其中n_i是G的次数,$k_i=|G:C_G(g_i)|$是g_i所在共轭类的元素个数,χ_1是主特征标.

定理3.7.1　如果α是G的一个线性特征标,χ是C的一个不可约特征标,则$\alpha\chi$是G的一个不可约特征标.

证明　因为α是线性的,由定理3.6.4(3)得,$\alpha(g)$是单位根,其中$g\in G$.特别地,对于$\forall\ g\in G$,$1=|\alpha(g)|=\alpha(g)\overline{\alpha(g)}$,由行正交定理,我们有

$$
\begin{aligned}
(\alpha\chi,\alpha\chi) &= \frac{1}{|G|}\sum_{g\in G}\alpha(g)\chi(g)\,\overline{\alpha(g)\chi(g)} \\
&= \frac{1}{|G|}\sum_{g\in G}\chi(g)\,\overline{\chi(g)}\alpha(g)\,\overline{\alpha(g)} \\
&= \frac{1}{|G|}\sum_{g\in G}\chi(g)\,\overline{\chi(g)}=(\chi,\chi)=1.
\end{aligned}
$$

再由推论3.6.3知$\alpha\chi$是不可约的.

列正交定理　如果$g_1,\cdots,g_r$是G的共轭类的代表元,$k_1,\cdots,k_r$分别是这些共轭类

的元素个数，则对任意的 $1 \leqslant i,j \leqslant r$，我们有

$$\sum_{t=1}^{r} \chi_t(g_i)\,\overline{\chi_t(g_j)} = \frac{|G|}{k_i}\delta_{ij} = |C_G(g_i)|\delta_{ij}.$$

证明 设 $\Gamma = (\chi_i(g_j))$，$1 \leqslant i,j \leqslant r$ 是 G 的特征标表，K 是 $r \times r$ 对角矩阵，其对角线元素为 $(k_1,\cdots,k_r)$，则对任意的 i 和 j，我们有

$$(\Gamma K)_{ij} = \sum_{l=1}^{r} \chi_i(g_l)(K)_{lj} = \chi_i(g_j),$$

于是对 $\forall\ i$ 和 j 来说，由行正交性我们有

$$\begin{aligned}(\Gamma K \overline{\Gamma}') &= \sum_{l=1}^{r} \chi_i(g_l) k_l (\overline{\Gamma}')_{lj} = \sum_{l=1}^{r} k_l \chi_i(g_l)\,\overline{\chi_j(g_l)} \\ &= \sum_{g \in G} \chi_i(g)\,\overline{\chi_j(g)} = |G|(\chi_i,\chi_j) = |G|\delta_{ij},\end{aligned}$$

其中 $\overline{\Gamma}'$ 是 $\overline{\Gamma}$ 的转置，故 $\Gamma K \overline{\Gamma}' = |G|I$，其中 I 是 r 阶单位阵. 可以验证如果 A 和 B 是两个满足 AB 是非零的数量矩阵，则 $AB = BA$. 利用这个事实可得 $K\overline{\Gamma}'\Gamma = |G|I$. 因而对任意的 i 和 j，我们有

$$G|\delta_{ij} = \sum_{l=1}^{r} (K\,\overline{\Gamma}')_j \Gamma_{li} = \sum_{l=1}^{r} k_j\,\overline{\chi_l(g_j)}\chi_l(g_i).$$

后面我们要研究一个群的表示理论与它的商群的表示理论之间的关系.

引理 3.7.2 设 $N \lhd G$，U 是一个 $C(G/N)$ 模，则 U 也是一个 CG 模. U 的一个子空间是一个 CG 子模当且仅当它是一个 $C(G/N)$ 子模. 若 ψ 是 $C(G/N)$ 模 U 的一个特征标，则 CG 模 U 的特征标是 $\psi\eta$，其中 $\eta: G \to G/N$ 是一个自然同态.

证明 给定 $N \lhd G$，$u \in U$，定义 $gu = (gN)_u$，则 U 是一个 CG 模，且 U 的 CG 子模恰好就是 U 的 $C(G/N)$ 子模. 又从 $gu = (gN)_u$ 可知，G 在 U 上的作用与 G/N 在 U 上的作用是相同的，从而对任意的 $g \in G$，g 在 U 上诱导的线性变换与 $\eta(g) = gN$ 在 U 上诱导的线性变换是相同的，由特征标的定义即得所证结论.

对 G 的任一特征标 χ，令 $K_\chi = (x \in G \mid \chi(x) = \chi(1))$，由定理 3.5.4 可知，$K_\chi \lhd G$，$K_\chi$ 称为 χ 的核. 经常把 K_{χ_i} 简记为 K_i.

定理 3.7.3 设 $N \lhd G$，则 $N = \bigcap_{i \in I} K_i$，其中 $I \subseteq (1,\cdots,r)$. 特别地，$\bigcap_{i=1}^{r} K_i = 1$.

证明 设 $N \lhd G$，$U = C(G/N)$，令 ψ 是 $C(G/N)$ 模 U 的特征标，χ 是 CG 模 U 的特征标，因为 ψ 是 G/N 的正则特征标，由引理 3.6.6 得，$\chi(g) = \chi(1)$ 当且仅当 $g \in N$，故 $K_\chi = N$. 令 $\chi = \Sigma_i a_i \chi_i$，其中 a_i 是非负整数，则对于 $\forall\ g \in G$，由定理 3.6.4(5) 得到

$$|\chi(g)| \leqslant \Sigma_i a_i |\chi_i(g)| \leqslant \Sigma_i a_i \chi_i(1) = \chi(1),$$

由这些不等式及定理 3.6.4(5) 又得 $g \in K_\chi$ 当且仅当对每个使得 $a_i > 0$ 的 i，都有 $g \in K_i$，因而 $N = \bigcap_{i \in I} K_i$，其中 $I = \{1 \leqslant i \leqslant r \mid a_i > 0\}$.

反之，因为对每个 i 来说，$K_i \lhd G$，从而 $\bigcap_{i\in I}K_i \lhd G$，其中 $I\subseteq(1,\cdots,r)$. 设 ρ 是 G 的正则特征标，则对任意的 $\chi\in\mathrm{Irr}(G)$，我们有

$$(\rho,\chi)=\frac{1}{|G|}\rho(1)\chi(1)=\chi(1),$$

于是 $\rho=\Sigma\chi(1)\chi$，其中 $\chi\in\mathrm{Irr}(G)$. 若 $g\in\bigcap_{i=1}^{r}K_i$，则 $\rho(g)=\Sigma\chi(1)\chi(g)=\Sigma\chi(1)^2\neq 0$，于是 $g=1$.

定理 3.7.4 G 是单群当且仅当对某个 $1\neq g\in G$，使得 $\chi_i(g)=\chi_i(1)$ 的 G 的某个不可约特征标 χ_i 只能是主特征标 χ_1.

证明 设 G 是单群，且存在 G 的一个非单位元 g，使得对 G 的某个不可约特征标 χ_i 来说 $\chi_i(g)=\chi_i(1)$，则一定有 χ_i 为主特征标，否则，定有 K_i 为 G 的非平凡正规子群，矛盾.

反之，若 G 不是单群，则存在某个 $1\neq g\in G$ 使得 $g\in N\lhd G$，由定理 3.6.7 知，存在某个 $i>1$ 使 $N\leqslant K_i$，因为 K_i 是 χ_i 的核，故 $\chi_i(g)=\chi_i(1)$，而对 $g\in C/N$，定有 $\chi_i(g)\neq\chi_i(1)$，这与 χ_i 是主特征标相矛盾，故 χ_i 只能是主特征标 χ_1.

定理 3.7.5 G 的特征标表可以用于判断 G 是否为可解群.

证明 由定理 3.6.7 知，G 的特征标表使得我们能确定 G 的所有正规子群以及这些正规于群之间的包含关系，因而可确定 G 的所有的正规列以及正规列中每项的阶. 特别地，我们可确定 G 是否有一个正规列且其相邻两群的商群为 p 群. 由此即可判断 G 是否为可解群. 对于 G 的特征标 χ，定义 $Z_\chi=\{x\in G\,|\,\chi(x)=\chi(1)\}$，经常把 Z_{χ_i} 简记为 Z_i.

引理 3.7.6 设 χ 是 G 的特征标，$Z_\chi\leqslant C$，而且 χ 是不可约的，则

$$Z_\chi/K_\chi=Z(C/K_\chi).$$

证明 设 $g\in G$，由定理 3.6.4(4) 知，若 $g\in Z_\chi$，则 $g^{-1}\in Z_\chi$. 再由定理 3.6.4(3) 知，$\chi(g)$ 是 $\chi(1)$ 个单位根的和. 因而 $|\chi(g)|=\chi(1)$ 当且仅当 g 恰好有一个特征值. 如果 $g\in Z_\chi$，令 $\lambda(g)$ 是 g 的特征值，若 U 是与 χ 相对应的 CG 模，则对 $\forall\ u\in U$，我们有 $gu=\lambda(g)u$. 由此可知，若 $g,h\in Z_\chi$，则对 $\forall\ u\in U$，我们有 $(gh)u=\lambda(g)\lambda(h)u$，因而 $\chi(gh)=\chi(1)\lambda(g)\lambda(h)$，由此得 $|\chi(gh)|=\chi(1)$，也即 $gh\in Z_\chi$. $Z_\chi\leqslant G$.

设 $\psi:G\to GL(U)$ 是与 χ 相对应的表示，则对 $\forall\ g\in Z\chi$，$\psi(g)$ 在 U 的任何一个基下对应的矩阵是数量矩阵，因而 $\psi(g)\in Z(\psi(G))$. 因为 $\psi(G)\cong G/K_\chi$，故 $Z_\chi/K_\chi\leqslant Z(G/K_\chi)$. 设 χ 是不可约的，若 $gK_\chi\in Z(G/K_\chi)$，则对任意的 $x\in G$ 来说，$\psi(g)\psi(x)=\psi(x)\psi(g)$，因而映射 $u\longmapsto gu$，$u\in U$ 是 CG 模 U 的一个自同态. 因为 χ 是不可约的，故 U 是单模，由 Schur 引理得 $\mathrm{End}_{CG}(U)\cong C$.

这意味着存在一个复单位根 ω 使得对任意的 $u\in U$ 都有 $gu=\omega u$. 于是我们有 $\chi(g)=\chi(1)u$，由此得 $|\chi(g)|=\chi(1)$，因而 $g\in\mathbf{Z}_\chi$. 综上所述

$$Z_\chi/K_\chi = Z(C/K_\chi).$$

引理 3.7.7 若 G 是非交换单群,则对任意的 $i>1$ 都有 $Z_i=1$,

证明 若 $i>1$,则 $K_i=1$,由引理 3.6.10 即得,$Z_i=Z(G)=1$.

定理 3.7.8 $Z(G)=\bigcap_{i=1}^{r} Z_i$.

证明 设 χ 是 G 的特征标,则

$$Z(G)K_\chi/K_\chi \leqslant Z(G/K_\chi), Z(G)K_\chi/K_\chi \leqslant Z_i/K_i,$$

因而对每个 i 来说,$Z(G)\leqslant Z_i$.

反之,设对 $\forall\, i$ 来说,$g\in Z_i$,因为 $Z_i/K_i=Z(G/K_i)$,由此得知,对 $\forall\, i$ 以及 $x\in G$ 来说,又由命题 3.6.7 知,$K_1\cap\cdots\cap K_r=1$. 故对 $\forall\, x\in G$,都有$[g,x]=1$,因而 $gt\in Z(G)$,结论得证.

定理 3.7.9 设 $N\lhd G$,则 G/N 的不可约特征标可以由 G 的不可约特征标来确定.

证明 设 χ 是 G 的不可约特征标,N 含在其核中. 令 U 是与 χ 对应的单 CG 平凡地作用在 U 上,故对于 $gN\in G/N, u\in U$,若令$(gN)u=gu$,则 U 也是一个 $C(G/N)$ 模. 因为 U 是单 CG 模,故 U 也是一个单 $C(G/N)$ 模,且单 $C(G/N)$ 模 U 的特征标是 $gN\longmapsto\chi(g)$. 这就是说,核包含 N 的 G 的那些特征标也是 G/N 的特征标.

另一方面,G/N 的每个不可约特征标也给出 G 的核包含 N 的一个不可约特征标,因而 G/N 的不可约特征标可由 G 的不可约特征标来确定.

推论 3.7.10 G 的特征标表可以用于判断 G 是否为幂零群.

证明 考虑 G 的上中心列 $1\leqslant Z_1\leqslant Z_2\leqslant\cdots$,对每个 i 来说,我们有

$$Z_i\lhd G, Z_i/Z_{i-1}=Z(G/Z_{i-1}).$$

由定理 3.7.8 知每个 Z_i 可由 G/Z_{i-1} 的不可约特征标来确定.

因为每个 G/Z_{i-1} 的不可约特征标可由 G 的特征标表来确定,因而我们可由 G 的特征标表来确定 G 的上中心列的每一项. 由此可判断 G 是否为幂零群.

由推论 3.7.10 的论证过程可知,若 G 为幂零群,则由 G 的特征标表可以确定 G 的幂零类.

问题 3.7

1. 计算 $|\Gamma|$.

2. 证明:Γ 中任意一行元素之和为非负整数.

3. 设 G 依照共轭变换作用在 G 上,计算 G 集 G 的特征标,确定不可约特征标的乘法.

4. 设 χ 是 G 的不可约特征标,$I\in CG$ 是 CG 看为 CG 代数时它的直和分解中某一项

的恒等元，证明：$I = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g$.

5. 设 $N \lhd G$ 且 $g \in G$，证明：$|C_G(g)| \geqslant |C_{G/N}(gN)|$.

§3.8　群的特征标的例子

由以上讨论看出，有限群 G 的特征标在研究有限群 G 时有很大的作用. 下面通过例子来探讨寻找特征标的方法，并用这些方法来构造群的特征标表.

例 3.8.1　设 $G = \langle g\rangle \cong Z_n$，其中 $1 \neq n \in \mathbf{N}$，令 λ 是一个 n 次单位根，对于 $\forall\ 1 \leqslant i \leqslant n$，令 V_i 是复数域 C 上的一维向量空间. 对于 $g \in G, v \in V_i$，令 $gv = \lambda^{i-1}v$，因为 G 是循环的，易知 V_i 作成一个 CG 模. 因为每个 V_i 是一维的，故 V_i 是单 CG 模. 若 χ_i 是 V_i 的特征标，则 $\chi_i(g) = \lambda^{i-1}$，从而对 $\forall\ a$ 来说，$\chi_i(g^a) = \lambda^{a(i-1)}$，因为 $\chi_1, \cdots, \chi_n$ 是 G 的 n 个不同的线性特征标，而 G 至多有 $|G|$ 个不可约特征标，故 $\chi_i(1 \leqslant i \leqslant n)$ 恰好是 G 的所有不可约特征标，于是 G 的特征标表为

	1	1	1	1
	1	g	g^2	g^{lr1}
χ_1	1	1	1	1
χ_2	1	λ	λ^2	λ^{lr1}
χ_3	1	λ^2	λ^4	λ^{lr2}
χ_4	1	λ^{lr1}	λ^{lr2}	λ

由上表看出，G 的 n 个特征标在特征标的乘法运算下作成一个循环群，其生成元为 χ^2，且对 $\forall\ i$ 来说，$\chi_i = \chi_2^{i-1}$.

例 3.8.2　设 G 和 H 是群，其不可约特征标分别为 $\chi_1, \cdots, \chi_r$ 及 $\psi_1, \cdots, \psi_s$. 下面我们确定 $G \times H$ 的不可约特征标. 我们知道，$G \times H$ 的两个元素 (x, y) 与 (x', y') 是共轭的当且仅当 x 和 x' 在 G 中共轭以及 y 与 y' 在 G 中共轭. 又 G 和 H 分别有 r 和 s 个共轭类，由此 $G \times H$ 有 rs 个共轭类，且这 rs 个共轭类是由 G 的 r 个共轭类与 H 的 s 个共轭类相乘得到，因而 $G \times H$ 有 rs 个不可约特征标.

设 $S_1, \cdots, S_r$ 与 $T_1, \cdots, T_s$ 分别是不同的单 CG 模与单 CH 模，对 $\forall\ i$ 和 $j, g \in G, s \in S_i, t \in T_j$，令 $(g, h)(s \odot t) = gs \odot ht$ 并作线性扩张，则 $S_i \odot T_j$ 作成一个 $C(G \times H)$ 模. 对 $\forall\ i$ 和 j，令 δ_{ij} 是 $S_i \odot T_j$ 的特征标. 由此可知 $\delta_{ij}(g, h) = \chi_i(g)\psi_j(h)$，记 $\delta_{ij} = \chi_i \times \psi_j$，我们看到，$\delta_{ij}$ 是互不相同的，且通过适当的限制我们可由 δ_{ij} 重新获得 χ_i 和 ψ_j，于是对 $\forall\ i, i', j, j'$ 由行正交性我们有

$$(\delta_{ij}, \delta_{i'j'}) = \frac{1}{|G \times H|}\sum_{(g,h)\in(G\times H)}\delta_{ij}(g)\,\overline{\delta_{i'j'}(g,h)}$$

$$= \frac{1}{|G||H|}\sum_{g\in G}\sum_{h\in H}\chi_i(g)\psi_j(h)\overline{\chi_{i'}(g)\psi_{j'}(h)}$$
$$= \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\overline{\chi_{i'}(g)}\frac{1}{|H|}\sum_{h\in H}\psi_j(h)\overline{\psi_{j'}(h)}$$
$$= (\chi_i,\chi_{i'})(\psi_j,\psi_{j'}) = \delta_{ij}\delta_{i'j'}.$$

特别地，对 $\forall\ i$ 和 j，有 $(\delta_{ij},\delta_{ij})=1$，由推论 3.6.3 可知 δ_{ij} 是不可约特征标，是 $G\times H$ 的 rs 个不可约特征标，也即 $G\times H$ 的不可约特征标的集合是 $\{\chi_i\times\psi_j\}_{i,j}$.

例 3.8.3 设 G 是交换群，则 G 的每个共轭类只有一个元素组成. 由定理 3.5.3 知 G 有 $|G|$ 个不可约特征标，又由推论 3.6.2 知，$\sum_{i=1}^{|G|}n_i^2=|G|$.

因而对每个 i，必有 $n_i=1$，也即 G 的所有不可约特征标都是线性的. 又 G 是循环 p 群的直积. 令这些循环 p 群的生成元为 $g_1,\cdots,g_t$，其阶分别为 $p_1^{a_1},\cdots,p_t^{a_t}$，由例 3.6.1 和例 3.6.2 我们可由这些循环 p 群的特征标来确定 G 的特征标.

我们知道 G 的一个线性特征标 χ 恰好是 G 到复数乘群 C^* 的一个同态，因而为了确定 χ，只要对每个 i 确定 $\chi(g_i)$ 即可. 而 $\chi(g_i)$ 是一个 $p_i^{a_i}$ 次单位根，因而 G 的不可约特征标与 t 元有序数组 $(\lambda_1,\cdots,\lambda_t)$ 之间有一个一一对应，其中 λ_i 是一个 $p_i^{a_i}$ 次单位根.

作为一个简单的例子，令 $G=\langle a,b\rangle\cong Z_2\times Z_2$，则 a 和 b 都是 2 阶元，由上我们知道 G 的 4 个不可约特征标对应于 2 元有序数组：

$$(1,1),(1,-1),(-1,1),(-1,-1).$$

于是 G 的特征标表是

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

表中的第二列和第三列与上面的 2 元有序数组相对应，而第四列完全可由前两列确定.

例 3.8.4 由 G/G' 是交换群知，G/G' 的不可约特征标都是线性的，而引理 3.6.6 告诉我们，由 G/G' 的每一个线性特征标都可得到 G 的一个线性特征标，且由 G/G' 的不同的线性特征标都可得到 G 的不同的线性特征标. 设 χ 是 G 的线性特征标，则 $\chi:G\to C^*$ 是一个同态. 设其同态核为 K_χ，于是 G/K_χ 是交换群，且知 $G'\leqslant K_\chi$，因而我们可定义 G/G' 的线性特征标 ψ 为 $\psi(gG')=\chi(g)$，$g\in G$. 这样 G 的每一个线性特征标 χ 都可由 G/G' 的一个线性特征标 ψ 得到.

例 3.8.5　考虑 S_3 的特征标表，已知 S_3 有三个共轭类 $\{1\}$，$\{(12),(13),(23)\}$，$\{(123),(132)\}$. 又 $S'_3 = A_3$ 且 $S_3/A_3 \cong Z_2$，故 S_3 有两个线性特征标. 由引理 3.6.6 知它们可由 Z_2 的特征标得到. 令 χ_1,χ_2 是 S_3 的两个特征标，则我们有

	1	3	2
	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3			

由推论 3.6.2 知

$$6 = |S_3| = n_1^2 + n_2^2 + n_3^2 = 2 + n_3^2$$

由此得 $n_3 = 2$. 由列正交性得

$$0 = \sum_1^3 n_i\chi_i((1,2)) = 1\times 1 + 1\times(-1) + 2\chi_3((12)),$$

$$0 = \sum_1^3 n_i\chi_i((1,2,3)) = 1\times 1 + 1\times 1 + 2\chi_3((123)),$$

由此得 S_3 的特征标表为

	1	3	2
	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

例 3.8.6　设 G 是 8 阶非交换群，则我们可决定 G 的特征标表，因为 8 阶非交换群有两个同构类，这个例子说明，不同构的群可能有相同的特征标表，换句话说，一个特征标表不能完全确定一个群.

已知 $|Z(G)| = 2$，因而 $Z(G) \cong Z_2$. 因为 G 是非交换群，故 $G/Z(G)$ 是 4 阶交换群且非循环群. 又 $G' = Z(G)$，这样 $G/G' \cong Z_2\times Z_2$，由例 3.8.3 和例 3.8.4 知 G 恰有 4 个线性特征标. 由推论 3.6.2，我们有 $\sum_{i=1}^{r} n_i^2 = 8$，其中 $1\leqslant i\leqslant 4, n_i = 1$，对于 $i > 4, n_i > 1$. 这就使 $r = 5$ 且 $n_5 = 2$. 设 x 是 G' 的生成元，因为 $G' = Z(G)$，故 1 和 x 恰在 G 的两个不同的单元素共轭类中，因而其余三个共轭类的元素个数均为 2. 令 a,b 和 c 分别是这三个共轭类的代表元，因为 G/G' 也有 4 个共轭类，所以 a,b 和 c 在 G/G' 中像必在不同的共轭类中，利用例 3.6.3 中 $Z_2\times Z_2$ 的特征标表，我们可获得 G 的部分特征标表：

	1	1	2	2	2
	1	x	a	b	c
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2				

又由列正交性，我们得 $\chi_5(a)=\chi_5(b)=\chi_5(c)=0$，以及 $\chi_5(x)=-2$，这就完成了 G 的特征标表.

例 3.8.7　考虑 A_5 的特征标表.

已知 A_5 元素在 S_5 中有 4 个共轭类，这 4 个共轭类的代表元为 1，(12)(34)，(123)，(12345). 这 4 个共轭类的元素个数 k_i 分别为 1，15，20，24.

注意到 A_5 的元素在 S_5 中共轭，但不一定在 A_5 中共轭.

设 $x\in A_5$，K 表示 x 在 S_5 中的共轭类，则 $|K|=|S_5:C_{S_5}(x)|$. 而 x 在 A_5 中的共轭类含在 K 中，且其阶为 $|A_5:C_{A_5}(x)|$. 设 $C_{S_5}(x)$ 不包含于 A_5，因为 A_5 是 S_5 的极大子群，故必有 $A_5C_{S_5}(x)=S_5$. 由群的第一同构定理，我们有

$$S_5/A_5=A_5C_{S_5}(x)/A_5\cong C_{S_5}(x)/(A_5\cap C_{S_5}(x))=C_{S_5}(x)C_{S_5}(x)/C_{A_5}(x)$$

因而 $|A_5:C_{A_5}(x)|=|S_5:C_{A_5}(x)|/|S_5:A_5|$

$$=|S_5:C_{A_5}(x)|/|C_{S_5}(x):C_{A_5}(x)|=|S_5:C_{S_5}(x)|=|K|$$

在这种情况下，K 与 x 在 A_5 中的共轭类相等.

设 $C_{S_5}(x)\leqslant A_5$，则我们有 $C_{A_5}(x)=C_{S_5}(x)\cap A_5=C_{S_5}(x)$，因而 $|A_5:C_{A_5}(x)|=|A_5:C_{S_5}(x)|=1/2|S_5:C_{S_5}(x)|=1/2K$.

在这种情况下，K 是 x 在 A_5 中的两个元素个数相等的共轭类的并集.

容易看出，1，(12)(34)，(123) 均与 S_5 中的某个奇置换可交换. 因而这三个元素在 A_5 中的共轭类也是在 S_5 中的共轭类. 因为 24 不整除 60，所以(12345) 在 S_5 中的共轭类在 A_5 中是两个元素个数相等的共轭类的并集，因而 A_5 的共轭类的元素个数 k_i 分别为 1，15，20，12，12. 我们首先证明 $x=(12345)$ 与 $x^2=(13524)$ 在 S_5 中是不共轭的，从而 x 在 S_5 中的共轭类在 A_5 中有两个共轭类，其中一个含有 x，另一个含有 x^2. 设 $g\in A_5$ 使得 $gxg^{-1}=x^2$，则 $g\langle x\rangle g^{-1}=\langle x^2\rangle=\langle x\rangle$. 因而 $g\in N_{A_5}(x)$，又 $\langle x\rangle\in \mathrm{Syl}_5(A_5)$，又 A_5 有 6 个 Sylow5 子群，于是 $|N_{A_5}(\langle x\rangle)|=10$. 通过观察有 $N_{A_5}(\langle x\rangle)=\langle x\rangle\times\langle t\rangle\cong D_{10}$，其中 D_{10} 为二面体群，$t=(25)(43)$. 但是 $txt^{-1}=x^{-1}\neq x^2$，可见，不存在 $g\in N_{A_5}(\langle x\rangle)$，使得 $gxg^{-1}=x^2$，矛盾. 故 x 与 x^2 在 A_5 中不共轭.

由上证明知 A_5 有 5 个共轭类，代表元为 1，(12)(34)，(123)，(12345)，(13524). 这 5

个共轭类的元素个数k_i分别为1,15,20,12,12.因为A_5是单群,我们不可能像前面的例子那样,由A_5的商群的不可约特征标来获得A_5的不可约特征标.然而,由于A_5是置换群,我们可用置换所具有的特点来确定A_5的特征标表.

设$X=\{1,2,3,4,5\}$,由例3.6.4知,$\pi(g)$等于$g\in A_5$作用在X上不动点的个数,因而我们有

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
π	5	1	2	0	0
$\pi-\chi_1$	4	0	1	-1	-1

另一方面,我们又有$(\pi-\chi_1,\pi-\chi_1)=\dfrac{1}{|A_5|}\sum\limits_{i=1}^{5}k_i[(\pi-\chi_1)(g_i)]^2=\dfrac{1}{60}\times(1\times 16+15\times 0+20\times 1+12\times 1+12\times 1)=1$.

由推论3.6.3知,$\pi-\chi_1$是不可约特征标,令$\chi_2=\pi-\chi_1$.

设Y是X的二元子集组成的集合,则Y是一个传递的A_5集.令ψ是CA_5模CY的特征标,则我们又有

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
ψ	5	1	2	0	0
$\psi-\chi_1$	4	0	1	-1	-1

另一方面,$(\psi-\chi_1,\psi-\chi_1)=\dfrac{1}{|A_5|}\sum\limits_{i=1}^{5}k_i[(\psi-\chi_1)(g_i)]^2=\dfrac{1}{60}(1\times 81+15\times 1+20\times 0+12\times 1+12\times 1)=2$.

由推论3.6.8知,$\psi-\chi_1$是两个不可约特征标的和,因为Y是传递的A_5集,就像例3.8.4所作的那样,这两个不可约特征标都不等于χ_1.我们又有

$$\begin{aligned}(\psi-\chi_1,\chi_2)&=\frac{1}{|A_5|}\sum_{i=1}^{5}k_i(\psi-\chi_1)\chi_2(g)\\&=\frac{1}{60}(1\times 9\times 4+15\times 1\times 0+20\times 0\times 1+24\times(-1)\times(-1))\\&=1,\end{aligned}$$

因而由推论3.6.4知,$(\psi-\chi_1-\chi_2)$是一个特征标,它既不等于χ_1,也不等于χ_2.

令$\chi_3=\psi-\chi_1-\chi_2$,我们有$n_3=5$,又由推论3.5.2得:$\sum\limits_{1}^{5}n_i^2=|A_5|=60$.由此$n_4^2+n_5^2=18$,从而$n_4=n_5=3$.这样我们就得到$A_5$的部分特征标表(见下页):

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3				
χ_5	3				

令 $a=\chi_4((12)(34)), b=\chi_5((12)(34))$，由列正交性，我们有

$$0=\sum_1^5 n_i\chi_i((1,2)(3,4))=1\times 1+4\times 0+5\times 1+3a+3b,$$

因而 $a+b=-2$，由命题 3.6.4(3) 知，a 和 b 均为三个单位平方根之和，故 $a,b\in\{-3,-1,1,3\}$. 但由列正交性，我们有

$$4=60/15=|A_5|/k_2=\sum_1^5|\chi_i((1,2)(3,4))|^2=1+0+1+a^2+b^2;$$

由此得 $a^2+b^2=2$，从而 $a=b=-1$. 再由列正交性，我们又有

$$3=60/20=|A_5|/k_3=\sum_1^5|\chi_i((1,2,3))|^2$$
$$=1+1+1+|\chi_4((123))|^2+|\chi_5((123))|^2;$$

于是 $|\chi_4((123))|^2+|\chi_5((123))|^2=0$，因而得出 $\chi_4((123))=\chi_5((123))=0$；又有下列 A_5 的部分特征标表：

	1	15	20	12	12
	1	(12)(34)	(123)	(12345)	(13524)
χ_1	1	1	1	1	1
χ_2	4	0	1	-1	-1
χ_3	5	1	-1	0	0
χ_4	3	-1	0		
χ_5	3	-1	0		

令 $x=(12345)$，上面我们证明 x 与 x^2 在 A_5 中不共轭时发现 x 与 x^{-1} 在 A_5 中是共轭的，因而 $\chi_4(x)=\chi_4(x^{-1})$. 由定理 3.6.4(4) 可知，$\chi_4(x)$ 是实数，类似的论证可知，$\chi_4(x^2),\chi_5(x)$ 及 $\chi_5(x^2)$ 也是实数.

令 $c=\chi_4(x), d=\chi_4(x^2)$，由行正交性，我们有

$$0=\sum_1^5 n_i\chi_4(g_i)=1\times 3+15\times(-1)+20\times 0+12c+12d$$

由此得 $c+d=1$，因为 $\chi_4(x^2)$ 也是实数，我们又有

$$60=\sum_{1}^{5}n_i\chi_4(g_i)^2=1\times 9+15\times 1+20\times 0+12c^2+12d^2$$

由此又得 $c^2+d^2=3$，因而 $c^2-c-1=0$. 不失一般性，我们设

$$c=\frac{1+\sqrt{5}}{2}\text{ 及 } d=1-c=\frac{1-\sqrt{5}}{2}$$

类似有

$$\chi_5(x)=\frac{1-\sqrt{5}}{2};\chi_5(x^2)=\frac{1+\sqrt{5}}{2}.$$

这就完全确定了 A_5 的特征标表.

问题 3.8

1. 设 G 双传递地作用在 X 上，证明：CX 的特征标是主特征标与其他不可约特征标的和.

2. 对任意的 $n\in\mathbf{N}$，确定 D_{2n} 的特征标表.

3. 确定 S_5 的特征标表.

4. 设 $N\lhd G$，ψ 是 G/N 的特征标，定义 $\chi:G\to C$，其中 $\chi(g)=\psi(gN)$，则

(1) χ 是 G 的特征标；(2) $\chi\in\mathrm{Irr}(G)$ 当且仅当 $\psi\in\mathrm{Irr}(G/N)$.

5. 设 $N\lhd G$，χ 是 G 的一个不可约特征标，$N\subseteq K_\chi$，证明：

(1) 存在 $\psi\in\mathrm{Irr}(G/N)$ 使得对任意的 $g\in G$ 都有 $\chi(g)=\psi(gN)$；

(2) $|G:N|=\sum_{\chi\in K}\chi(1)^2$，其中 $K=\{\chi\in\mathrm{Irr}(G)\mid N\subseteq(K_\chi)\}$.

§3.9　有限群特征标理论的应用

最后，我们给出有限群特征标理论的初步应用.

Burnide 定理　p^aq^b 阶群是可解群，其中 p,q 是不同的素数，a,b 是正整数.

Frobenius 定理　设 G 是有限群，$H\leqslant G$，对 $\forall\ g\in G-H$ 都有 $H\cap H^g=1$，则 $N=\{x\in G|x$ 与 H 的任何元素都不共轭$\}\cup\{1\}$ 是 G 的正规子群，进一步有 $G=HN$，$N\cap H=1$.

Frobenius 定理中的群 G 称为 Frobenius 群，H 称为 Frobenius 补，N 称为 Frobenius 核. 设 χ 是 G 的特征标，$H\leqslant G$，令 $\chi_H:H\to C$ 是 χ 限制到 H 上得到的一个函数. 因为 G 的表示限制到 H 上产生一个 H 的表示，因而 χ_H 是 H 的一个特征标，即 $\chi_H\in cf(H)$.

定义 3.9.1　设 $\varphi\in cf(H)$，$a\in G$，定义 $\varphi^G(a)=\frac{1}{|H|}\sum_{g\in G}\varphi^0(gag^{-1})$

其中 $\varphi^{\circ}: G \to C$ 满足 $\varphi^{\circ}(H) = \begin{cases} \varphi(h), h \in H \\ 0, \cdots h \notin H \end{cases}$，$\varphi^{G}$ 称为 φ 在 G 上的诱导类函数.

事实上，若 a 与 b 在 G 中共轭，设 $b = xax^{-1}$，则

$$\varphi^{G}(b) = \frac{1}{|H|}\sum_{g\in G}\varphi^{\circ}(gbg^{-1})$$
$$= \frac{1}{|H|}\sum_{g\in G}\varphi^{\circ}(gxa(gx)^{-1}) = \frac{1}{|H|}\sum_{g\in G}\varphi^{\circ}(gag^{-1}) = \varphi^{G}(a),$$

这说明 φ^{G} 确为 G 的类函数，即 $\varphi^{G} \in cf(G)$. 若 $h = G$，显然有 $\varphi^{\circ} = \varphi$，从而 $\varphi^{G} = \varphi$. 又由定义可得 $\varphi^{G}(1) = |G:H|\varphi(1)$.

Frobenius 互反律 设 $H \leqslant G, \varphi \in cf(H), \psi \in cf(G)$，则 $(\varphi^{G}, \psi) = (\varphi, \psi_{H})$.

证明 直接计算可得

$$(\varphi^{G}, \psi) = \frac{1}{|G|}\sum_{g\in G}\varphi^{G}(g)\overline{\psi(g)} = \frac{1}{|G||H|}\sum_{g\in G}\sum_{x\in G}\varphi^{\circ}(xgx^{-1})\overline{\psi(g)}$$
$$= \frac{1}{|G||H|}\sum_{y\in G}\sum_{x\in G}\varphi^{\circ}(y)\overline{\psi(x^{-1}gx)} = \frac{1}{|H|}\sum_{y\in H}\varphi(y)\overline{\psi(y)} = (\varphi, \psi_{H}).$$

推论 3.9.1 设 $H \leqslant G$，若 φ 是 H 的特征标，则 φ^{G} 也是 G 的特征标.

证明 因为 $\varphi^{G}(1) = |G:H|\varphi(1)$，故 $\varphi^{G} \neq 0, \forall \chi \in \mathrm{Irr}(G)$，由 Frobenius 互反律知，$(\varphi^{G}, \chi) = (\varphi, \chi_{H})$，又知 (φ, χ_{H}) 是非负整数，从而 (φ^{G}, χ) 也是非负整数. 再据定理 3.6.4 得 φ^{G} 是 G 的特征标.

引理 3.9.2 设 G 是 Frobenius 群，$H \leqslant G$ 是 G 的 Frobenius 补，若 $\varphi, \psi \in cf(H)$，$\varphi(1) = 0$，则 $(\varphi^{G})_{H} = \varphi$，且 $(\psi, \varphi) = (\psi^{G}, \varphi^{G})$.

证明 设 $h \in H$，我们只需证 $\varphi^{G}(h) = \varphi(h)$. 若 $h = 1$，则 $\varphi^{G}(1) = |G:H|\varphi(1)$，从而 $\varphi^{G}(1) = \varphi(1)$. 不妨设 $h \neq 1$，则

$$\varphi^{G}(h) = \frac{1}{|H|}\sum_{x\in G}\varphi^{\circ}(xhx^{-1})$$

若 $x \notin H$，则 $H \cap H^{x} = 1$，由此得 $h \notin H$. 在这种情况下，$\varphi^{\circ}(xhx^{-1}) = 0$，于是

$$\varphi^{G}(h) = \frac{1}{|H|}\sum_{x\in G}\varphi^{\circ}(xhx^{-1}) = \varphi(h)$$

对于第二个结论，由 Frobenius 互反律及上面的结论可知，

$$(\psi, \varphi) = (\psi, (\varphi^{G})_{H}) = (\psi^{G}, \varphi^{G})$$

引理 3.9.3 设 G 是 Frobenius 群，$H \leqslant G$ 是 G 的 Frobenius 补，$\chi \in \mathrm{Irr}(H)$，令 $N = \{x \in G \mid x$ 与 H 任何元素都不共轭$\}$，则存在 $\chi^{*} \in \mathrm{Irr}(G)$ 使得 $\chi^{*}_{H} = \chi$ 且 $N \subseteq K_{\chi^{*}}$.

证明 若 $\chi = 1_{H}$ 是 H 的主特征标，则我们取 $\chi^{*} = 1_{G}$，此时我们有 $\chi^{*}_{H} = \chi$ 且 $N \subseteq G = K_{\chi^{*}}$. 不妨设 $\chi \neq 1_{H}$ 且定义 $\varphi = \chi^{*} - \chi(1)1_{H} \in cf(H)$，则显然有 $\varphi(1) = 0$. 由推论 3.9.1 知，$\varphi^{G} \in cf(G)$，于是 φ^{G} 是 $\mathrm{Irr}(G)$ 中元素的 $\mathbf{Z}$ 线性组合. 又由 Frobenius 互

反律可得$(\varphi^G,1_G)=(\varphi,1_H)=-\chi(1)$.

不妨设$\varphi^G=\chi^*-\chi(1)1_G$,其中$\chi^*\in cf(G)$是$G$的除了主特征标$1_G$以外的其他不可约特征标的$\mathbf{Z}$线性组合.由此可得$(\varphi^G,\varphi^G)=(\chi^*,\chi^*)+\chi(1)^2$.

另一方面,$(\varphi^G,\varphi^G)=(\varphi,\varphi)=(\chi,\chi)+\chi(1)=1+\chi(1)^2$.比较两式可得$(\chi^*,\chi^*)=1$.

设$\chi^*=\Sigma_{\psi\in\mathrm{Irr}(G)}a_\psi\psi$,其中$a_\psi\in\mathbf{Z}$,则$1=(\chi^*,\chi^*)=\Sigma a_\psi^2$.由此可知,对某个$\psi\in\mathrm{Irr}(G)$,我们有$\chi^*=\pm\psi$,又由引理3.9.2得$(\varphi^G)_H=\varphi$,于是$(\chi^*-\chi(1)1_G)_H=\chi-\chi(1)1_H$,由此可得$(\chi^*)_H=\chi$.

特别地,$\chi^*(1)=\chi(1)>0$,这说明$\chi^*\neq-\psi$,从而$\chi^*=\psi\in\mathrm{Irr}(G)$.

对于第二个结论,令$g\in\mathbf{N}$,由诱导类函数的定义,直接计算可得$0=\varphi^G(g)=\chi^*(g)-\chi(1)$,于是$\chi^*(g1)=\chi(1)$,故$g\in K_\chi$.

Frobenius 定理的证明 令$N=\{x\in G|\ x$与H的任何元素都不共轭$\}\cup\{1\}$,也即$N=(G-\bigcup_{g\in G}H^g)\cup\{1\}$.

对$\forall\chi\in\mathrm{Irr}(H)$,令$\chi^*\in\mathrm{Irr}(G)$同引理3.9.3所设.对所有的$\chi\in\mathrm{Irr}(H)$都有$N\subseteq K_{\chi^*}$.令$M=\bigcap K_{\chi^*}$,其中$\chi$取遍$\mathrm{Irr}(H)$的每个元素,由命题3.6.7知$M$是包含$N$的$G$的正规子群,又由引理3.9.3知$\chi_H^*=\chi$,再由命题3.7.3得$M\cap H=\bigcap K_{\chi^*}=1$.

又从$M\cap H=1,M\lhd G$我们得到对所有$g\in G,M\cap H^g=1$,于是$M\subseteq N$,从而$N=M$是G的正规子群.

下证$G=NH$.由题设$N_G(H)=H,H$有$|G:H|$个互不相交的共轭子群,由此得

$$|N|=|G|-|\bigcup_{g\in G}(H^g-1)|=|G|-|G:H|(|H|-1)=|G:H|.$$

因为$N\cap H=1$,我们有

$$|NH|=|N||H|=|G:H||H|=|G|,\text{故 }G=NH.$$

最后证明 Burnside 定理,为此需要有关代数整数的概念,$a\in\mathbf{C}$称为代数整数,若存在一个首项系数为1的多项式$f(x)\in\mathbf{Z}[x]$使得$f(a)=0$.

引理 3.9.4 若a是有理数且为代数整数,则a必为整数.

证明 设$a/b\in\mathbf{Q}$是代数整数,其中$(a,b)=1,1\neq b\in\mathbf{N}$,则对某个$n\in\mathbf{N}$使得

$$(\frac{a}{b})^n+c_{n-1}(\frac{a}{b})^{n-1}+\cdots+c_1(\frac{a}{b})+c_0=0$$

用b^n乘等式的两边,我们有$a^n\equiv0(\mathrm{mod}\,b)$,与$a,b$互素相矛盾.

引理 3.9.5 设$\alpha\in\mathbf{C}$,则α是代数整数当且仅当$\mathbf{Z}[\alpha]$是有限生成$\mathbf{Z}$-模,其中$\mathbf{Z}[\alpha]$是整数环$\mathbf{Z}$上关于α的多项式环.

证明 设α适合的$\mathbf{Z}[\alpha]$中的整系数多项式为$x^n+a_{n-1}x^{n-1}+\cdots+a_0$,于是$\alpha^n$

$= -(a_{n-1}\alpha^{n-1}+\cdots+a_0)$，故 α^n 以及 α 的更高次幂均可由 $1,\alpha,\cdots,\alpha^{n-1}$ 线性表出，且表达式的系数均为整数. 这说明 $1,\alpha,\cdots,\alpha^{n-1}$ 是 $\mathbf{Z}[\alpha]$ 的一个生成元集，即 $\mathbf{Z}\{\alpha\}$ 是有限生成模.

反之，设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 $\mathbf{Z}[\alpha]$ 的一个生成元集，则对 $\forall\ a, a\alpha_i$ 是 $\mathbf{Z}$ 线性组合，即 $a\alpha_i=\sum_{j=1}^{n}a_{ij}\alpha_j, a_{ij}\in\mathbf{Z}$，整理得

$$0=\sum_{j=1}^{n}(a_{ij}-\delta_{ij}\alpha)\alpha_j, i=1,2,\cdots,n,$$

其中 δ_{ij} 是 Kronecker 符号. 因为上述齐次线性方程组有非零解 $\alpha_1,\alpha_2,\cdots,\alpha_n$，故系数矩阵的行列式必为零. 故 α 是多项式 $\det((a_{ij})-xI))$ 的根.

因为这个多项式的系数可能为 -1，但适当变换后可使它的首项系数为 1，即 α 为代数整数.

定理 3.9.6　所有的代数整数关于数的加法和乘法构成一个环.

证明　设 α,β 是代数整数，由引理 3.9.5 知，$\mathbf{Z}[\alpha]$，$\mathbf{Z}[\beta]$ 是有限生成模，设 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，$\{\beta_1,\beta_2,\cdots,\beta_n\}$ 分别是 $Z[\alpha]$ 与 $\mathbf{Z}[\beta]$ 的一个生成元集，验算可知，$\alpha_i\beta_j, 1\leqslant i\leqslant n$，$1\leqslant j\leqslant m$ 是 $\mathbf{Z}[\alpha\beta]=\mathbf{Z}[\alpha][\beta]$ 的一个生成元集，即 $\mathbf{Z}[\alpha,\beta]$ 是有限生成的. 因为 $\mathbf{Z}$ 是主理想环，又 $\mathbf{Z}[\alpha\pm\beta]$ 与 $\mathbf{Z}[\alpha\beta]$ 都是 $\mathbf{Z}[\alpha,\beta]$ 的子模，所以 $\mathbf{Z}[\alpha\pm\beta]$ 与 $\mathbf{Z}[\alpha\beta]$ 都是有限生成模，且 $\alpha\pm\beta,\alpha\beta$ 都是代数整数，从而所有代数整数构成一个环.

代数整数与有限群表示理论的联系体现在下列基本事实中：

引理 3.9.7　设 χ 是 G 的一个特征标，则对 $\forall\ g\in G,\chi(g)$ 是代数整数.

证明　设 $g\in G$，知 $\chi(g)$ 是一些单位根的和，而单位根是代数整数，由定理 5.9.6 得 $\chi(g)$ 是代数整数.

引理 3.9.8　设 $\chi\in\mathrm{Irr}(G), g\in G$，则 $|G:C_G(g)|\ \chi(g)/\chi(1)$ 是代数整数.

证明　设 S 是单 CG 模，其对应的特征标是 χ. 令 $g\in G$，K 是 g 所在的共轭类，$\alpha=\Sigma_{x\in K}x\in CG$. 考虑 S 到 S 的映射 $\varphi: s\longmapsto\alpha s, s\in S$，由定理 3.5.3 的证明可知 α 在 CG 的中心里，由此得 $\varphi\in\mathrm{End}_{CG}(S)$. 由 Schur 引理知，存在 $\lambda\in C$ 使得对所有 $s\in S$ 都有 $\alpha s=\lambda s$，计算迹我们有

$$\lambda\chi(1)=\sum_{x\in K}\chi(x)=|K|\chi(g)=|G:C_G(g)|\chi(G),$$

因而

$$\lambda=|G:C_G(g)|\chi(g)/\chi(1).$$

考虑 CG 到 CG 的映射 $\sigma: y\longmapsto y\alpha, y\in CG$. 由引理 3.3.11 知，$\sigma\in\mathrm{End}_{CG}(CG)$，因为 S 是单 CG 模，则 S 可看作是 CG 模的子模，又 α 在 CG 的中心里，故对任意的 $0\neq s\in S\subseteq CG$，我们有 $\sigma(s)=s\alpha=\alpha s=\lambda s$，这说明 $\lambda\sigma$ 的特征值.

于是若令 A 是 σ 对于 C 上的向量空间 CG 在基 G 下的矩阵，则我们有 $\det(\lambda I - A) = 0$.

另一方面，A 的元素是 0 或 1，由此可得 $f(\lambda) = \mathrm{der}(\lambda I - A)$ 是系数在 $\mathbf{Z}$ 中的首项系数为 1 的关于 λ 的多项式. 因为 $f(\lambda) = 0$，故 λ 是代数整数.

引理 3.9.9　设 $\chi \in \mathrm{Irr}(G)$，则 $\chi(1) \mid |G|$.

证明　设 $g_1, \cdots, g_n$ 是 G 的共轭类的代表元，由引理 3.9.7，3.9.8 及定理 3.6.4(4) 知对 $\forall\, i$，$|G : C_G(g) \mid \chi(g)/\chi(1)$ 和 $\overline{\chi(g_i)}$ 是代数整数. 由行正交定理有

$$\frac{|G|}{\chi(1)} = \frac{1}{\chi(1)} \sum_{i=1}^{k} |G : C_G(g_i)| \chi(g) \overline{\chi(g_i)}$$

$$= \sum_{i=1}^{k} (|G : C_G(g_i)| \chi(g)/\chi(1) \cdot \overline{\chi(g_i)}).$$

由定理 3.9.6 知是代数整数，又由引理 3.8.4 即得结论.

引理 3.9.10　设 $\chi \in \mathrm{Irr}(C)$，K 是 G 的一个共轭类，$(|K|, \chi(1)) = 1$，对于 $g \in K$，令 $\alpha = \chi(g)/\chi(1)$，则 $\alpha = 0$ 或 $|\alpha| = 1$.

证明　存在 $s, t \in \mathbf{Z}$ 使得 $s|K| + t\chi(1) = 1$，于是 $s|K|\chi(g) + t\chi(1)\chi(g) = \chi(g)$. 用 $\chi(1)$ 除上式的两边，由引理 3.9.7 和 3.9.8 可知：

$$\chi(g) \text{ 和 } \frac{|K|\chi(g)}{\chi(1)} \text{ 均为代数整数，}$$

因而 $\dfrac{\chi(g)}{\chi(1)}$ 也是代数整数.

令 $\dfrac{\chi(g)}{\chi(1)} = \lambda = \lambda_1, \lambda_2, \cdots, \lambda_n$ 为 λ_1 适合的 $\mathbf{Q}$ 上极小多项式的所有共轭根. 由定理 3.6.4(3) 知 $\chi(g) = \sum_{i=1}^{\chi(1)} \omega_i$ 各单位根的和，其中 $\omega_i i$ 是 n 次单位根. 于是

$$\lambda_1 = \sum_{i=1}^{\chi(1)} \frac{\omega_i}{\chi(1)},$$

从而每个 λ_i 都可写成 $\dfrac{\omega_i}{\chi(1)}$ 这样一些数的和. 由此可知对 $\forall\, i$ 来说，$|\lambda_i| \leqslant 1$.

令 $a = \prod_{i=1}^{n} \lambda_i$，则 $a \in \mathbf{Q}$ 且 a 是代数整数（$\pm\, a$ 就是 λ_1 所适合的 $\mathbf{Q}$ 上极小多项式的常数项）. 由引理 3.9.4 知 $a \in \mathbf{Z}$，但是 $|a| = \prod_{i=1}^{n} |\lambda_i| \leqslant 1$，故 $a = 0, \pm 1$. 因为所有的 λ 是共轭的，从而 $a = 0 \Leftrightarrow \lambda_1 = 0 \Leftrightarrow \chi(g) = 0$.

另一方面，$a = \pm 1 \Leftrightarrow |\lambda_i| = 1$，对 $\forall\, i$，于是有 $a = 0$ 或 $|a| = 1$.

定理 3.9.11　若有限群 G 有一个共轭类的元素个数是素数的正方幂，则 G 不是单

群.

证明　设 G 是单群，$1 \neq g \in G$ 所在的共轭类 K 的元素个数为 p^n，p 是素数，$n \in \mathbf{N}$，亦即 $|K| = |G : C_G(g)| = p^n$，此时 G 不是交换群. 由列正交定理我们有

$$0 = \frac{1}{p}\sum_{i=1}^{r}\chi_i(g)\varphi_i(1) = \frac{1}{p} + \sum_{i=1}^{r}\frac{\chi_i(g)\chi_i(1)}{p}.$$

其中，$\chi_1, \chi_2, \cdots, \chi_r$ 是 G 的不可约特征标，由引理 3.9.4 知 $1/p$ 不是代数整数. 于是由定理 3.9.6 知对某个 $2 \leqslant i \leqslant r$，$\chi_i(g)\chi_i(1)/p$ 不是代数整数，因为 $\chi_i(g)$ 是代数整数，这说明 p 不整除 $\chi_i(1)$ 且 $\chi_i(g) \neq 0$. 又 $(|K|, \chi(1)) = 1$，于是存在 $a, b \in \mathbf{Z}$ 使得 $a|K| + b\chi(1)) = 1$，因而

$$\chi_i(g)/\chi_i(1) = a|G : C_G(g)|\ \chi_i(g)/\chi_i(1) + b\chi_i(g),$$

由引理 3.9.7 和 3.9.8 知，这是一个代数整数. 又 $|\chi_i(g)| = |\chi_i(1)|$，由此得

$$g \in \mathbf{Z}_i = \{x \in G\ |\chi_i(x) = \chi_i(1)\},$$

但 $\mathbf{Z}_i = 1$，矛盾. 故结论成立.

Burnside 定理的证明　设 G 是使定理不成立的极小反例，则 G 为单群，否则 G 有非平凡正规子群 N. 由 G 的极小性，必有 N 及 G/N 均可解，从而 G 可解. 令 $P \in \mathrm{Syl}_p(G)$，$1 \neq z \in Z(P)$，则 z 所在的共轭类元素个数必为 q 的正方幂，与定理 3.9.11 矛盾，故结论成立.

问题 3.9

1. 若 $H \leqslant G$，ψ 是 H 的特征标，证明：$Z(\psi^G) \leqslant H$.
2. 若 $H, K \leqslant G$ 且 $G = HK$，$\varphi \in cf(H)$，证明：$(\varphi^G)_K = (\Phi_{H\cap K})$.
3. 若 $H \leqslant G$，$|G : H| = n$，X 是 G 的一个特征标，证明：

(1) $(\chi, \chi) \geqslant (\chi_H, \chi_H)/n$；

(2) 若 H 是交换群，$\chi \in \mathrm{Irr}(G)$，则 $\chi(1) \leqslant n$；

(3) 若(2)中的等式成立，则 $H \lhd G$.

(4) 若 G 为奇阶群，则值为实数的不可约 H 是交换群，$\chi \in \mathrm{Irr}(G)$，$\chi(1) \leqslant n$.

4. 若 G 为奇阶群，证明：值为实数的不可约特征标只能是主特征标.

§3.10　有限群的不等价不可约表示

在本节以实例演示有限群不等价不可约表示的寻找方法. 首先根据上述几节所叙基本原理，构造群的特征标表，进而确定群的不等价不可约表示及其维数，再根据群元的具体含义以确定每个表示的具体形式.

试以 C_{4v} 群为例说明之.

1. 确定群的不等价不可约表示的维数

确定群的共轭类的个数 K,就是确定群的全部不可约表示的个数 c,即 $K = c$.

群 $C_{4v} = \{E, C_4^1, C_4^2, C_4^3, m_X, m_Y, \sigma_u, \sigma_v\}$ 可分为 5 类,即 $K = 5$,

$$e_1 = \{E\}, e_2 = \{C_4^1, C_4^3\}, e_3 = \{C_4^2\}, e_4 = \{m_X, m_Y\}, e_5 = \{\sigma_u, \sigma_v\}.$$

由此可见群 C_{4v} 有 5 个不等价不可约表示.

再由伯恩塞德定理 $\sum_{i=1}^{c} l_i^2 = g$,现在 $g = 8, c = 5$. 此时整数解只有

$$l_1 = l_2 = l_3 = l_4 = 1(\text{一维}), l_2 = 2\ (\text{二维}).$$

例 3.10.1　设 G 为 8 个元素构成的 Abel 群,求其全部不可约表示的个数及相应维数.

$g = 8$,共轭类个数 $K = 8$,即不等价不可约表示的个数 $c = 8$,由伯氏定理,$l_1 = l_2 = \cdots = l_8 = 1$,即全部为一维表示.

2. 构造特征标表

一般可以利用如下关系:

(1) 任何群的不可约表示 i:$\chi_i(E) = l_i$.

(2) 任何群 G 均存在平庸一维表示:$\Gamma^{(1)}(g_a) = 1(\forall\ g_a \in G)$.

(3) 一维表示就是其特征标,其乘法关系与群元间的乘法关系一致.

(4) 对于一维表示,若 $g_a^n = E$,则 $\chi^{(1)}(g_a) 1^{\frac{1}{n}} = e^{i2k\pi/n}$.

(5) 两个特征标正交关系.

(6) 不可约判据 $\sum_{k=1}^{c} n_k |\chi_k|^2 = g$.

例 3.10.2　n 阶循环群 $G = \{E, a, \cdots, a^{n-1}, a^n = E\}$,群的阶 $g = n$. 它是阿贝尔群,故 $c = K = g, l_1 = l_2 = \cdots = l_8 = 1$ 全部是一维表示.

由于 $a^n = E$,故 $\Gamma(E) = \Gamma(a^n) = 1$,即$[\Gamma(a)]^n = 1$,就是

$$\Gamma(a) = 1^{\frac{1}{n}} = e^{i2k\pi/n}(k = 0, 1, \cdots, n-1).$$

这样得到 n 个不同的表示:

令

$$\Gamma^{(p)}(a) = e^{2\pi i(p-1)/n}(p = 1, \cdots, n),$$

共轭类

$$e_1 = \{E\}, e_2 = \{a\}, \cdots, e_n = \{a^{n-1}\}.$$

对于 $\chi \in e_m$，应有

$$\Gamma^{(p)}(x) = \Gamma^{(p)}(a^{m-1}) = [\Gamma^{(p)}(a)]^{m-1} = [e^{2\pi i/n}]^{(p-1)(m-1)}$$

其中 p 为不可约表示序数，m 为共轭类的序数. 其特征标 $\chi_p^{(m)}$ 亦等于此数，$\chi_p^{(m)} = [e^{2\pi i/n}]^{(p-1)(m-1)}$，此群的特征标表如表 3.1（令 $n = 5$）所示.

表 3.1 循环群 $G = \{E, a, \cdots, a^{n-1}, a^n = E\}$ 特征标表

类元素 m / 不可约表示 p	e_1 (E)	e_2 (a)	e_3 a^2	e_4 a^3	e_5 a^4
$\chi_1^{(m)}$	1	1	1	1	1
$\chi_2^{(m)}$	1	$e^{2\pi i/5}$	$e^{4\pi i/5}$	$e^{6\pi i/5}$	$e^{8\pi i/5}$
$\chi_3^{(m)}$	1	$e^{4\pi i/5}$	$e^{8\pi i/5}$	$e^{12\pi i/5}$	$e^{2\pi i/5}$
$\chi_4^{(m)}$	1	$e^{6\pi i/5}$	$e^{12\pi i/5}$	$e^{18\pi i/5}$	$e^{30\pi i/5}$
$\chi_5^{(m)}$	1	$e^{8\pi i/5}$	$e^{20\pi i/5}$	$e^{30\pi i/5}$	$e^{32\pi i/5}$

例 3.10.3 构造 C_{4v} 群的特征标表。

C_{4v} 群的特征标表如表 3.2 所示。

表 3.2 C_{4v} 群的特征标表

类脚标 k / 表示脚标 i	e_1 $\{E\}$	e_2 $\{C_4^1, C_4^3\}$	e_3 $\{C_4^2\}$	e_4 $\{m_X, m_Y\}$	e_5 $\{\sigma_\mu, \sigma_v\}$
$\chi_1^{(k)}$	1	1	1	1	1
$\chi_2^{(k)}$	1	1	1	-1	-1
$\chi_3^{(k)}$	1	-1	1	1	-1
$\chi_4^{(k)}$	1	-1	1	-1	1
$\chi_5^{(k)}$	2	0	-2	0	0

演算过程如下：

(1) 由 $\chi_i(E) = l_i$ 和恒等表示，可以填出表中第一行与第一列；

(2) 考虑第三列，$l_3 = \{C_4^2\}$. 由于 $[C_4^2]^2 = E$，由例 3.10.2 得

$$\chi_2^{(3)}(C_4^2) = \pm 1, \chi_3^{(3)}(C_4^2) = \pm 1, \chi_4^{(3)}(C_4^2) = \pm 1.$$

但由 $\chi_i^{(2)}(C_4^1) = \chi_i^{(2)}(C_4^3) = [\chi_i^{(2)}(C_4^1)]^3$（第二列）可知

$$[\chi_i^{(2)}(C_4^1)]^2 = 1 = [\chi_i^{(2)}(C_4^1)]^3 \pm 1,$$

即 $\chi_i^{(3)}(C_4^2) = 1, \chi_i^{(2)} = \pm 1$；

(3) 由特征标第二正交定理得 $\sum_i \chi_i^{(k)} \chi_i^{(k')} = \frac{g}{n_k}\delta_{kk'}$，令 $K = 1$（l_1 类），$k' = 3$（l_3 类），注意 $n_1 = 1, n_3 = 2$，可得 $\chi_5^{(3)} = -2$；

(4) 对于 $i = 5$，由不可约表示依据：$\sum n_k |\chi_i^{(k)}|^2 = g$ $(g = 8)$，注意到 $n_1 = 1, n_2 =$

$2, n_{31}=1, n_{43}=2, n_{51}=1$，得 $\chi_5^{(2)}=\chi_5^{(2)}=\chi_5^{(5)}=0$；

(5) 由于 $m_X^2=m_Y^2=\sigma_\mu^2=\sigma_\nu^2=E$，得 $\chi_i^{(4)}=\pm 1, \chi_i^{(5)}=\pm 1$，由于序号选择的任意性，表示 $i=1,2,3,4$ 对应三种等价选择，只取一种就可以了．令 $\chi_2^{(4)}=-1, \chi_3^{(4)}=1, \chi_4^{(4)}=-1$，则 $\chi_2^{(5)}=-1, \chi_3^{(5)}=1, \chi_4^{(5)}=-1$．

例 3.10.4　$C_{3v}=\{E, C_3^1, C_3^2, m_a, m_b, m_c\}$．

$g=6$，由伯恩塞德定理得 $g=\sum_i l_i^2$，有 $l_1=l_2=1, l_3=2$，有三个不等价表示，两个一维的：

$$\chi_1^{(1)}(E)=1, \chi_2^{(2)}(E)=1, \chi_3^{(1)}=2.$$

此外，$\chi_1^{(1)}=\chi_2^{(2)}=\chi_3^{(1)}=1$(平凡表示)．

由同态定理 $G/N\sim G$，商群的不等价不可约表示系群 G 的不等价不可约的非忠实表示．令 $N=G$，则 G/N 为一阶群，对应平凡恒等表示

$$\{\Gamma^{(1)}(g_a)\}=\chi_1^a=1, \forall\ g_a\in G.$$

令 $N=\{E, C_3^1, C_3^2\}$，则 G/N 为二阶群，除平凡表示外，还有一个反对称表示 $\chi_1^{(1)}=1, \chi_2^{(2)}=-1$(可以一般证明，从略)．因为是一维表示，表示矩阵即为其特征标．

当 m 维不可约表示($m>1$)有 n 个时，如习题中 C_{5v} 群．设 $\{\Gamma^{(i)}\}$ 为群的一维表示，$\{\Gamma^{(j)}\}$ 是群的 m 维表示，则 $\{\Gamma^{(j)*}\}$ 与 $\{\Gamma^{(i)}\Gamma^{(j)}\}$ 亦为群 G 的 m 维表示，特征标为 $\chi^{(k)}{}_j^*=1$ 和 $\chi_i^{(k)}\chi_j^{(k)}$．m 维表示只有一个不等价不可约时，特征标必为实数，必为自共轭表示，即特征标全为实数．此时当 $\chi_i^{(k)}\neq 1$ 时，$\chi_j^{(k)}=0$．C_{3v} 的特征标表如表 3.3 所示。

表 3.3　C_{3v} 的特征标表

类 k ／ 不可约表示 i	$\{E\}$ l_1	$\{C_3^1, C_3^2\}$ l_2	$\{m_a, m_b, m_c\}$ l_3
$\chi_1^{(k)}$	1	1	1
$\chi_2^{(k)}$	1	1	-1
$\chi_3^{(k)}$	2	-1	0

3. 确定表示的具体形式

原则上可以通过约化群的正则表示得到，但过程繁琐，因此往往需要使用适当技巧，直接找到不可约表示的具体形式．

(1) 矩阵群．利用自身表示，再通过下节介绍的“表示直乘的分解”方法，找到不可约表示．此时可以视其为线性空间坐标的齐次变换(被动观点)，然后定义坐标的函数的

变换算符，找到相应变换的不变函数空间，从而得到其忠实表示. 在李群中将详细讨论之.

(2) 抽象群. 先找到其忠实表示，然后利用(1)中矩阵群中应用的方法.

例 3.10.5　求 C_{4v} 群不等价不可约表示的具体形式.

建立坐标系. 设 $\forall g_a \in C_{4v}, g_a$ 为二维空间的变换：

$$\begin{pmatrix} x \\ y \end{pmatrix} \xrightarrow{g_a} \begin{pmatrix} x' \\ y' \end{pmatrix} = \Gamma(g_a)\begin{pmatrix} x \\ y \end{pmatrix}.$$

当 $g_a = E$ 时，$\begin{pmatrix} x \\ y \end{pmatrix} = \Gamma(E)\begin{pmatrix} x \\ y \end{pmatrix}$，显然，$\Gamma(E) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$；

当 $g_a = C_4^3$ 时，$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -y \\ x \end{pmatrix} = \Gamma(C_4^3)\begin{pmatrix} x \\ y \end{pmatrix} \Rightarrow \begin{pmatrix} -y \\ x \end{pmatrix} = \begin{pmatrix} \Gamma_{11}(C_4^3)x + \Gamma_{12}(C_4^3)y \\ \Gamma_{21}(C_4^3)x + \Gamma_{22}(C_4^3)y \end{pmatrix}$.

对比两边，得 $\Gamma_{11}(C_4^3)x = \Gamma_{22}(C_4^3) = 0, \Gamma_{21}(C_4^3) = 1$，即 $\Gamma(C_4^3) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

其余元素可以仿此得到. 由于 C_{4v} 群只有一个二维表示，也就是说，C_{4v} 群的全部不等价不可约表示都已找到，分别是

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, C_4^1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, C_4^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, C_4^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$m_X = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, m_Y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_\mu = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \sigma_\nu = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

例 3.10.6　异常群(Ambivalent group)的特征标 $\chi(g_a) = \chi^*(g_a)$. 异常群定义为对于某个 $\forall g \in G$，有 $g_a = g^{-1}g_a^{-1}g$(即每个共轭类中包含群元及其逆).

证明　对于 G 的任意表示

$$\Gamma(g_a) = \Gamma(g^{-1}g_a^{-1}g) = \Gamma(g^{-1})\Gamma(g_a^{-1})\Gamma(g),$$

因而

$$\chi(g_a) = Tr[\Gamma(g^{-1})\Gamma(g_a^{-1})\Gamma(g)] = Tr[\Gamma(g_a^{-1})] = \chi(g_a^{-1}),$$

但是 $\chi(g_a^{-1}) = \chi(g_a)^{-1}$，故 $\chi(g_a) = \chi^a(g_a)$.

二面体群 D_n、$SU(2)$ 是异常群，循环群 $SU(n)(n > 3)$ 则是非异常群的实例.

问题 3.10

1. 利用正则表示寻找 C_{3v} 群的全部不可约不等价表示.

2. 四元素集合 $\overline{Q} = \{1, i, j, k, \overline{1}, \overline{i}, \overline{j}, \overline{k}\}$，其中

$i^2 = j^2 = k^2 = -1, ij = -ji = k(i,j,k$ 循环$), \overline{1} = -1, \overline{i} = -i, \overline{j} = -j, \overline{k} = -k$，乘法 $\overline{i}i = \overline{j}j = \overline{k}k = 1, ji = \overline{k}$ 等. 证明 $\overline{Q}$ 构成一个群.

(1) 给出 $\overline{Q}$ 群的乘法表；

(2) $\overline{Q}$ 分为 5 个等价表,群为异常群;

(3) 寻找群 $\overline{Q}$ 的全部不等价不可约表示.

4. 给出 C_{5v} 对称性的全部操作元素集合;它们构成 C_{5v} 群. 寻找 C_{5v} 群全部不等价不可约表示.

5. 证明狄拉克的四维克里福特(Cliford)代数 $r_\mu r_\nu + r_\nu r_\mu = 2\delta_{\mu\nu}E(\mu,\nu = 1,2,3,4)$ 在矩阵乘法下构成群 $G = \{E,\overline{E},r_\mu r_\nu(\mu > \nu),\overline{r_\mu r_\nu}(\mu > \nu)r_5,\overline{r_5},r_5 r_\mu,\overline{r_5 r_\mu}\}$,其中 $r_5 = r_1 r_2 r_3 r_4$,及 $\forall\ g_a \in G,\overline{g_a} = -\ g_a$. 求其不变子群 N 及相应商群,寻找此群的全部不等价不可约表示.

§3.11　直积群的表示

1. 表示的直积

设 $\{\Gamma^{(a)}(g_a)\}$ 与 $\{\Gamma^{(b)}(g_a)\}$ 为群 G 的两个 p 维与 q 维表示,则可用矩阵直积的方式构造集合 $\{\Gamma(g_i)\} = \{\Gamma^{(a)}(g_i) \otimes \Gamma^{(b)}(g_i)\},\quad \forall\ g_i \in G$.

可以证明该集合构成群 G 的表示,称为直积表示.

$\Gamma^{(a)}(g_i) \otimes \Gamma^{(b)}(g_i)$ 可以显式地表为 $\Gamma^{(a)}_{ij}[\Gamma^{(b)}]$ 表示矩阵元(数)与矩阵 $\Gamma^{(b)}$ 相乘. 显然 $\Gamma(g_a)$ 为 $(p \times q) \times (p \times q)$ 矩阵. 其矩阵元可表示为

$$\Gamma(g_a)_{ma,m\beta} \equiv \Gamma^{(a)}(g_l)_{mn}\Gamma(g_t)_{a\beta}(m,n = 1,\cdots,q).$$

此外,有重要关系

$$\begin{aligned}
[\Gamma^{(a)}(g_l)\Gamma^{(b)}(g_t)] &= \sum_{i,j}\Gamma^{(a)}(g_t)_{ma,ij}\Gamma^{(b)}(g_i)_{ij,n\beta}\\
&= \sum_{i,j}[\Gamma^{(a)}(g_t)_{mi}\Gamma^{(a)}(g_l)_{aj}\Gamma^{(b)}(g_t)_{in}\Gamma^{(b)}(g_i)_{j\beta}]\\
&= \sum_{i,j}[\Gamma^{(a)}(g_t)_{mi}\Gamma^{(a)}(g_t)_{in}][\Gamma^{(b)}(g_l)_{aj}\Gamma^{(b)}(g_i)_{j\beta}]\\
&= \sum_{i,j}[\Gamma^{(a)}(g_l)\Gamma^{(a)}(g_t)]_{mn}[\Gamma^{(b)}(g_l)\Gamma^{(b)}(g_i)]_{a\beta}\\
&= \{[\Gamma^{(a)}(g_l)\Gamma^{(a)}(g_i)] \otimes [\Gamma^{(b)}(g_l)\Gamma^{(b)}(g_i)]\}_{ma,m\beta}\\
&\quad (m,n = 1,\cdots,p;\alpha,\beta = 1,\cdots,q).
\end{aligned}$$

亦即

$$\begin{aligned}
&[\Gamma^{(a)}(g_l) \otimes \Gamma^{(b)}(g_i)][\Gamma^{(a)}(g_i) \otimes \Gamma^{(b)}(g_i)]\\
&= [\Gamma^{(a)}(g_l)\Gamma^{(a)}(g_i)] \otimes [\Gamma^{(b)}(g_i)\Gamma^{(b)}(g_i)].
\end{aligned}$$

由此式易见 $\{\Gamma\}$ 也构成群 G 的一个表示:

$$\begin{aligned}
\Gamma(g_l)\Gamma(g_t) &= [\Gamma^{(a)}(g_l) \otimes \Gamma^{(b)}(g_l)][\Gamma^{(a)}(g_t) \otimes \Gamma^{(b)}(g_t)]\\
&= [\Gamma^{(a)}(g_l)\Gamma^{(a)}(g_t)] \otimes [\Gamma^{(b)}(g_l)\Gamma^{(b)}(g_t)]
\end{aligned}$$

$$= [\Gamma^{(a)}(g_l g_t)] \otimes [\Gamma^{(b)}(g_l g_t)] = \Gamma(g_l g_t).$$

例 3.11.1 设系统由两子系统构成，两子系统之间相互作用可以略去，且它们有共同的对称群 G，则两者的能量本征函数，构成群 G 的不变子空间 L_a 与 L_b. 这些本征函数各自按群 G 的特定不可约表示 $\{\Gamma^{(a)}\}$ 与 $\{\Gamma^{(b)}\}$ 变换，即

$$P_a \Psi_\mu^{(a)}(x) = \Psi_\mu^{(a)}(g_a^{-1}x) = \sum_\nu \Psi_\nu^{(a)}(x)\Gamma^{(a)}(g_a)_{\nu\mu},$$

$$P_a \Phi_\rho^{(b)}(x) = \Phi_\rho^{(a)}(g_a^{-1}x) = \sum_\lambda \Phi_\lambda^{(b)}(x)\Gamma^{(b)}(g_a)_{\lambda\rho}$$

其中 $\forall\ \Psi_\mu^{(a)}(x) \in L_a, \forall\ \Phi_\rho^{(b)}(x) \in L_b (\rho = 1, \cdots, n; \mu = 1, \cdots, m), \forall\ g_a \in G$，则系统的总波函数 $\Psi_{\mu\rho}^{[ab]} \equiv \Psi_\mu^{(a)}(x)\Phi_\rho^b(x)$，总共有 $m \times n$ 个，并且

$$\begin{aligned} P_a \Psi_{\mu\rho}^{(ab)} &= \Psi_{\mu\rho}^{(ab)}(g_a^{-1}x) \\ &= \sum_{\nu\lambda} \Psi_\nu^{(a)}(x)\Phi_\lambda^{(b)}(x)\Gamma^{(a)}(g_a)_{\nu\mu}\Gamma^{(b)}(g_a)_{\lambda\rho} \\ &= \sum_{\nu\lambda} \Psi_{\nu\lambda}^{(ab)} \cdot [\Gamma^{(a)}(g_a) \otimes \Gamma^{(b)}(g_a)]_{\nu\lambda,\mu\rho}, \end{aligned}$$

其中 $[\Gamma^{(a)}(g_a) \otimes \Gamma^{(b)}(g_a)]_{\nu\lambda,\mu\rho} = \Gamma^{(b)}(g_a)_{\nu\lambda,\mu\rho}$ 是表示 $\{\Gamma^{(a)}\}$ 与 $\{\Gamma^{(b)}\}$ 为直积表示的矩阵元. 如果把 $\{\Psi_\mu^{(a)}\}$ 与 $\{\Phi_\rho^{(b)}\}$ 分别视为线性空间 L_a 与 L_b 的基，则 $\{\Psi_{\mu\rho}^{(a)}\}$ 正好生成直积空间 $L \equiv L_a \otimes L_b$.

系统的总波函数 $\{\Psi_{\mu\rho}^{(ab)}\}$ 按群 G 的表示 $\{\Gamma^{(a)}\}$ 与 $\{\Gamma^{(b)}\}$ 为直积表示 $\{\Gamma^{(ab)}\}$ 变换.

直积表示的特性标有重要性质：

$$Tr[\Gamma(g_a)] = Tr[\Gamma^{(a)}(g_a)] \cdot Tr[\Gamma^{(b)}(g_a)],$$

或 $\quad \chi(g_a) = \chi^{(a)}(g_a)\chi^{(b)}(g_a), \qquad \forall\ g_a \in G.$

2. 直积表示的约化

设直积表示 $\{\Gamma(g_a)\}$ 可以约化为 $\Gamma(g_a) = \sum_{\otimes_i} m_i \Gamma^{(i)}(g_a), \forall\ g_a \in G$，则应有

$$m_i = \frac{1}{g}\sum_a \chi^{(i)^*}(g_a)\chi(g_a) = \frac{1}{g}\sum_a \chi^{(i)^*}(g_a)[\chi^a(g_a)\chi^b(g_a)].\ (g = pq)$$

例 3.11.2 设 C_{4v} 群的二维表示为 $\Gamma^{(5)}$，则

$$\Gamma^{(5)} \otimes \Gamma^{(5)} = \Gamma^{(1)} \otimes \Gamma^{(2)} \otimes \Gamma^{(3)} \otimes \Gamma^{(4)}.$$

在量子力学中，两个不可约表示的直积的约化，通常称为对称群 G 的克莱布西-戈登(Clebsch-Gordon)级数. 相应的相似变换(使表示幺正化)矩阵元素叫 C-G 系数. 常用的系数已制成 C-G 系数表，查阅十分方便.

3. 群的直积表示

设群 G 为群 H 与 K 所构成的直积群 $G = H \otimes K$. 现讨论 G 的表示与 H、K 的表

示有什么关系.

设 $\forall H_m \in H(m=1,2,\cdots,h)$, $\forall K_\alpha \in K(\alpha=1,\cdots,k)$,则 $\forall G_{m\alpha} \in G$ 有

$G_{m\alpha}=H_mK_\alpha$. 令 $H_mK_\alpha=H_i$, $K_\alpha K_\beta=K_\gamma$,

则有

$$G_{m\alpha}G_{n\beta}=(H_m,K_\alpha)(H_n,K_\beta)=(H_i,K_\gamma)=G_{i\gamma}\in G.$$

设 $\{\Gamma^{(p)}H_m\}$ 与 $\{\Gamma^{(q)}K_\alpha\}$ 为群 H 与 K 的两个表示,则

$$\Gamma^{(p)}(H_m)\Gamma^{(p)}(H_n)=\Gamma^{(p)}(H_i),\Gamma^{(q)}(K_\alpha)\Gamma^{(q)}(K_\beta)=\Gamma^{(q)}(K_\gamma).$$

相应的直积,并用到上节证明的矩阵直积公式,

$$\begin{aligned}\Gamma^{(p)}(H_i)\otimes\Gamma^{(q)}(K_\gamma)&=[\Gamma^{(p)}(H_m)\Gamma^{(p)}(H_n)]\otimes[\Gamma^{(q)}(K_\alpha)\Gamma^{(q)}(K_\beta)]\\&=[\Gamma^{(p)}(H_m)\otimes\Gamma^{(q)}(K_\alpha)][\Gamma^{(p)}(H_n)\otimes\Gamma^{(q)}(K_\beta)].\end{aligned}$$

令 $\Gamma^{(pq)}(G_{i\gamma})=\Gamma^{(p)}(H_i)\otimes\Gamma^{(q)}(K_\gamma)$,则上式变为

$$\Gamma^{(pq)}(G_{i\gamma})=\Gamma^{(pq)}(G_{m\alpha})\Gamma^{(pq)}(G_{n\beta}),$$

其中 $G_{m\alpha},G_{n\beta}\in G$, $G_{i\gamma}=G_{m\alpha}G_{n\beta}\in G$,故 $\{\Gamma^{(pq)}(G_{i\gamma})\}$ 也构成群的一个表示. 换言之,用群 H 与群 K 表示的直积,提供了直积群的表示的构造方法. 但并非直积群的所有表示都可以用这种方法提供.

进而讨论直积群的不等价不可约表示. 设 $\{\Gamma^{(p)}\}$ 与 $\{\Gamma^{(q)}\}$ 为群 H 与 K 的两个不可约表示,则其直积 $\{\Gamma^{(pq)}\}$ 是群 G 的一个表示,且它的特征标

$$\chi_{pq}(G_{i\gamma})=\chi_p(H_i)\chi_q(K_\gamma),$$

其中 $\chi^{(p)}(H_i)$ 与 $\chi^{(q)}(K_\gamma)$ 应满足不可约判据,

$$\sum_{\forall H_m\in H}\chi_p(H_m)\chi_p^*(H_m)=h,\ \sum_{\forall K_\gamma\in K}\chi_q(K_\gamma)\chi_q^*(K_\gamma)=k.$$

上面两式的两边分别相乘,得

$$\begin{aligned}hk=g(G\text{ 的阶})&=\sum_{\substack{H_m\in H\\K_\gamma\in K}}[\chi_p(H_m)\chi_q(K_\alpha)][\chi_p(H_m)\chi_q(K_\alpha)]^*\\&=\sum_{G_{m\alpha}\in G}\chi_{pq}(G_{m\alpha})\chi_{pq}(G_{m\alpha})^*.\end{aligned}$$

由此可见, $\{\Gamma^{(pq)}(G_{m\alpha})\}$ 构成群的不可约表示. 亦即,若 $\{\Gamma^{(p)}(H_m)\}$ 与 $\{\Gamma^{(q)}(K_\alpha)\}$ 为群 H 与 K 的不可约表示,则 $\{\Gamma^{(pq)}\}$ 构成直积群的不可约表示. 事实上用这种方法可以构成群 G 的全部不等价不可约表示.

由伯恩塞德定理,对于 $\{\Gamma^{(p)}\}$ 与 $\{\Gamma^{(q)}\}$,有

$$\sum_{i=1}^{c_h}l_{(i)}^2=h,\sum_{j=1}^{c_k}l_{(j)}^2=k.$$

相乘得

$$hk = g = \sum_{i=1}^{c_h}\sum_{j=1}^{c_k}[l_i l_j]^2,$$

其中 $l_i l_j = l_{ij}$ 就是群 G 的一个表示的维数，c_h 与 c_k 分别为群 H 与群 K 的全部不等价不可约表示的个数. 上式可改写为

$$\sum_{i,j} l_{ij}^2 = g.$$

由伯恩塞德定理可知，左边求和遍及所有群 G 的不等价不可约表示，

推论 3.11.1 直积群的全部共轭类数 c_g 等于 H 与 K 的共轭类数的乘积，即 $c_g = c_h \cdot c_k$.

用群 H 与 K 的表示直积的方法虽然不能构造群 G 的全部表示，但是用群 H 与 K 的所有不等价不可约表示构成的直积表示，却可提供全部不等价不可约表示.

例 3.11.3 Γ 矩阵群.

N 个矩阵满足对易关系 $\{\gamma_\mu,\gamma_\nu\} = \gamma_\mu\gamma_\nu + \gamma_\nu\gamma_\mu = 2\delta_{\mu\nu}I, \mu,\nu = 1,2,\cdots,N$. 由 γ_μ 矩阵以及一切可能连乘的集合构成 Γ 矩阵群.

γ_μ 矩阵性质：

$$\gamma_\mu^2 = 1;\gamma_\mu\gamma_\nu + \gamma_\nu\gamma_\mu = 0 \qquad (\mu \neq \nu).$$

对该群取一个忠实的自我不可约幺正表示：

$$\gamma_\mu^+ = \gamma_\mu^{-1} = \gamma_\mu$$

令 $\gamma_\eta = \gamma_1\gamma_2\cdots\gamma_N$，则 $\gamma_\eta^2 = (-1)^{N(N+1)/2}\gamma_\eta$. 当 N 为奇数时，γ_μ 与 $\gamma_\nu(\mu = 1,2,\cdots,N)$ 对易，因此由舒尔引理，γ_η 应为常数矩阵，即有

$$\gamma_\eta = \begin{cases} \pm E, & N = 4n+1, \\ \pm iE, & N = 4n-1. \end{cases} \text{(不是新元素)}$$

当 $N = 4n+1$ 与 $4n$ 时，两个矩阵群同构；当 $N = 4n-1$ 时，生成元为 $r_\mu(\mu = 1, 2,\cdots,N-2)$ 和 iE. 因此，$\{\Gamma(4n-1)\} = \{\Gamma(4n-2)\} \otimes \{E,iE\}$. 以后只需讨论 $N = 2n$ 的偶数 Γ 矩阵群，Γ 矩阵群 G 是异常群. $\forall\ g_a \in G, -g_a \in G$，设所有“+”号 g_a 构成集合 Γ'，其元素个数 $= g/2$. 集合 Γ' 的元素，即从 N 个 γ_μ 矩阵中取 m 个不同 γ_μ 矩阵 $(m = 1,2,\cdots,N)$ 乘积的数目应为

$$g/2 = C_N^0 + C_N^1 + C_N^2 + \cdots + C_N^m + \cdots + C_N^N = 2^N,$$

故群的阶

$$g = 2^{N+1}(N = 2n).$$

显然，其特征标在自身表示中，

$$\chi(g_a) = \begin{cases} \pm d & g_a = \pm I, \\ 0, & g_a \neq \pm I. \end{cases}$$

由不可约判别法

$$I=\frac{1}{g}\sum_{g_a\in G}|\chi(g_a)|^2=\frac{2d^2}{2^{N+1}},$$

故在最低维表示中的维数 $d=2^{N/2},N=2n$.

此外,

$$\det\gamma_\mu=(-1)^{d/2}(\text{当 }N\geqslant 4\text{ 时},\det\gamma_\mu=1).$$

由于 $\forall g_a\in\Gamma'$,有 $Tr\{\Gamma(g_a)\}=0$,所有 g_a 构成完备线性空间 L_d. 事实上,如果线性相关,$\sum_{g_a\in\Gamma'}C(g_a)g_a=0$ (系数 $C(g_a)$ 不全为零). 用 $g_i^{-1}\in\Gamma'$ 右乘此式,并取迹,得 $C(g_i)=0$. 仿此可证全部 $C(g_i)=0,\forall g_i\in\Gamma'$. 故任何 $d\times d$ 矩阵 M 均可按 g_a 展开,

$$M=\sum_{g_a\in\Gamma'}C(g_a)\cdot g_a,C(g_a)=\frac{1}{d}Tr(g_a^{-1}M).$$

一般说来,当 $N=4n$ 时,除一维表示外,Γ 矩阵群只有一个 d 维表示;当 $N=4n-1$ 时,有两个不等价不可约的 d 维表示. 可以证明,两组等价的 d 维不可约表示 r 矩阵,实际上只确定到一常数. 如限制相似变换矩阵的模为 1,则常系数取 $\exp(\mathrm{i}2\pi m/d)$,其中 $0\leqslant m\leqslant d$.

γ_μ 矩阵群的具体形式(自身表示):

(i)$N=2$,可取泡利矩阵和单位矩阵,

$$\gamma_1=\sigma_1,\quad\gamma_2=\sigma_2,\quad\gamma_3=-\mathrm{i}\gamma_1\gamma_2=\sigma_3,\quad I.$$

(ii)$N=2$ (狄拉克矩阵).

$$\gamma_1=\sigma_2\times\sigma_1,\gamma_2=\sigma_2\times\sigma_2,\gamma_3=\sigma_1\times I,\gamma_4=\sigma_2\times\sigma_3,\gamma_5=\sigma_3\times I=-\gamma_1\gamma_2\gamma_3\gamma_4.$$

$\{\Gamma\}$ 矩阵群在旋量分析、量子场论、高能粒子物理的分立对称(电荷共轭、CP 共轭)中有广泛应用.

Burnside 小传

伯恩赛德(W. Burnside),英国数学家,1852 年 7 月 2 日生于伦敦. 1871 年入剑桥圣约翰学院学习,1873 年转入彭布罗克学院. 1875—1886 年任研究员,1885 年起任格林尼治皇家海军学院数学教授,直至去世. 1893 年选为英国皇家学会会员,1906—1908 年任伦敦数学会会长. 前期主要研究应用数学,还研究椭圆函数以及微分几何等. 1892 年起研究群论,是群表示论的主要创始人之一,并应用群表示论证明 p^aq^b 阶群是可解群(p,q 为素数). 1899 年获伦敦数学会德·摩根奖. 他所著的《群论》(1897) 是有限群论的第一部系统著作,深刻影响其后的群论体系. 1900 年左右,Burnside 提出了一个著名的猜想:一个奇数阶群 G 必存在一个正规子群列:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\},$$

使得每个C_i/G_{i+1}是交换群.这一猜想对有限单群分类问题的研究起了重大作用.50多年后,猜想最终被费特(W. Feit)和汤普森(J. G. Thompson)在一篇长达255页的论文中所证明. Burnside的另一重要猜想是关于群$B_{m,n}$的.1994年,柴尔曼诺夫(E. I. Zelmanov)由于在这一猜想方面的工作而获得菲尔兹奖.

Burnside 1927年8月21日卒于西威克姆.

问题 3.11

1. 试证:在Γ矩阵群中,有关系式$\gamma_\eta^2 = (-1)^{N(N+1)/2}\gamma_\eta$,式中$\gamma_\eta = \gamma_1\gamma_2\cdots\gamma_N$.

2. 试证:$N = 4n$与$N = 4n+1$的两Γ矩阵群同构.

3. 证明:当$N = 2n$时,满足反对易关系$\{\gamma_\mu,\gamma_\nu\} = 2\delta_{\mu\nu}I$ $(\mu,\nu = 1,\cdots,N)$的两组d维不可约表示$\{\gamma_\mu\}$与$\{\gamma'_\mu\}$必等价,$\gamma'_\mu = X^{-1}\gamma_\mu X$(其中$X$为$d\times d$矩阵,$\det X \neq 0$)[提示:证明其特征标相同.注意到$\gamma_\mu$矩阵是零迹、厄米、幺正的,本征值为$\pm 1$,且成对出现,否则不会零迹,故$\chi'(\gamma'_\mu) = \chi(\gamma_\mu) = \begin{cases} \pm d, & \gamma_\mu = \pm I, \\ 0, & \gamma_\mu \neq \pm I. \end{cases}$

4. 证明:两循环群$G_1 = \{E,\sigma_\mu\}$与$G_2 = \{E,\sigma_\nu\}$(其中σ_μ与σ_ν为绕μ轴与ν轴转动180°,μ轴与ν轴同在一个平面上,且互相垂直)的直积群为$G_1\otimes G_2 = G = \{I,C_2^1,\sigma_\mu,\sigma_\nu\}$(其中$C_2^1$为绕$z$轴的旋转$\pi$),由$G_1$与$G_2$的不等价不可约表示构造群$G$的全部不等价不可约表示.

第 4 章　物理学中的对称群

本章介绍群的对称性在晶体物理及量子力学中的应用，主要涉及有限群论，同时还比较详细地介绍对称群与点群. 虽然这些内容限于对称群的初步应用，但足以证实，群的对称性在自然科学与工程技术中有无限光明的前景.

§ 4.1　Wigner-Eckart 定理

我们讨论定态波函数按对称群分类

$$P_a\Phi_\rho(x) = \Phi_\rho(g_a^{-1}x) = \sum_{\lambda=1}^{m}\Phi_\lambda(x)\Gamma(g_a)_{\lambda\rho},$$

式中 m 个本征函数 $\{\Phi_\rho(x)\}(\rho = 1,2,\cdots,m)$ 对应同一本征值，称为 m 重简并. $\{\Gamma(g_a)\}$ 称为对应能量 E 的表示. $\{\Phi_\rho(x)\}$ 构成希尔伯特空间中的不变子空间. 选取幺正幺模表示作为所有等价表示的标准形式，则可作如下约化：

$$\Gamma(g_a) = \sum_{\otimes i} m_i\Gamma^{(i)}(g_a), \forall\ g_a \in G$$

$$\chi(g_a) = \sum_{i} m_i\chi_i(g_a),$$

其中　$$m_i = \frac{1}{g}\sum_{\forall\ g_a\in G}\chi_i^*(g_a)\chi(g_a).$$

若 $\{\Gamma(g_a)\}$ 为非标准形式，可按照标准的线性代数方法对角化，即

$$\{\Gamma'(g_a)\} = X^{-1}\{\Gamma(g_a)\}X,$$

这相当于空间基矢 $\{\Phi_\rho(x)\}$ 变换到 $\{\Psi_\rho(x)\}$，其中 $\Psi_\rho^{(jr)} = \sum_\rho \Phi_\rho(x)X_{\rho\mu}^{(ir)}$，符号 i 表示约化 $\Gamma(g_a) = \sum_{\otimes i} m_i\Gamma^{(i)}(g_a)$ 式中所含的低维不可约序号，r 则表示按 $\{\Gamma^{(i)}(g_a)\}$ 表示变换的子函数集合 $\{\Phi_\mu^{(i)}\}$.

因此，若 P_a 表示元素对应的变换算符，则

$$P_a\Psi_\mu^{(ri)}(x) = \sum\Psi_\mu^{(ri)}(x)\Gamma^{(i)}(g_a)_{\mu\rho}, \forall\ g_a \in G$$

相应上式的逆变换是

$$\Phi_\rho(x) = \sum_{i\mu r} \Psi_\mu^{(ri)}(x)(X^{(ir)})_{\mu\rho}^{-1},$$

这里，$\Psi_\mu^{(ri)}(x)$ 称为属于不可约表示 $\{\Gamma^{(i)}(g_a)\}$ 的第 μ 行的函数.

令 $P_\mu^{(i)}$ 为作用在任意函数 $\Phi(x)$ 上，并可以把属于不可约表示 $\{\Gamma^{(i)}(g_a)\}$ 的第 μ 行函数挑选出来的投影算子. 令

$$P_\mu^{(i)} \equiv \frac{m_i}{g}\sum_{g_a\in G}\Gamma^{(i)*}(g_a)_{\mu\rho}P_a.$$

事实上，

$$\begin{aligned}
P_\mu^{(i)}\Phi_\rho(x) &= \sum_{i',\mu',r}\frac{m_i}{g}\sum_{g_a\in G}(\Gamma^{(i)*}(g_a)_{\mu\mu'})P_a\Psi_{\mu'}^{(ri')}(X^{(i'r)})_{\mu'\rho}^{(-1)} \\
&= \sum_{i',\mu',r}\frac{m_i}{g}\sum_{g_a\in G}(\Gamma^{(i)*}(g_a)_{\mu\mu'})\cdot\sum_{v}\Psi_v^{(i'r)}(x)\Gamma^{(i)}(g_a)_{v\mu'}(X^{(i'r)})_{\mu'\rho}^{-1} \\
&= \sum_{\gamma}\Psi_\mu^{(ir)}(x)(X^{(ir)})_{\mu\rho}^{-1}.
\end{aligned}$$

此式右边表示的确实是 $\Phi_\rho(x)$ 中属不可约表示 $\{\Gamma^{(i)}(g_a)\}$ 的第 μ 行的函数成分. 由上定义式，即

$$P^{(i)} = \sum_{\mu=1}^{m}P_\mu^{(i)} = \frac{m_i}{g}\sum_{g_a\in G}\chi_i^*(g_a)P_a,$$

$$P^{(i)}\Phi_\rho = \sum_{r,\mu}\Psi_\mu^{(ri)}(x)(X^{(ri)})_{\mu\rho}^{-1} = \sum_{i=1}^{n}\Phi_\rho^{(i)},$$

其中 $\{\Phi_\rho^{(i)}\}(i=1,2,\cdots,n)$ 属于不可约表示 $\{\Gamma^{(i)}(g_a)\}$ 的函数组. 容易证明由上两式所定义的投影算符满足完备性、正交性、等幂性.

Wigner-Eckart 定理　幺正线性变换群 P_c 的两个不等价不可约幺正表示的函数(行矢量)相互正交；同一不可约幺正表示不同行的函数(行矢量)正交，而同一行函数的内积(即模)与行序号无关.

证明　令(上、下标意义同上)

$$\begin{cases}
P_a\Psi_\mu^{(ri)}(x) = \sum_{\nu}\Psi_\nu^{(i)}\Gamma^{(i)}(g_a)_{\nu\mu}, \\
P_a\Psi_\mu^{(ri)}(x) = \sum_{\lambda}\Psi_\lambda^{(j)}\Gamma^{(j)}(g_a)_{\lambda\rho},
\end{cases}\qquad(\forall\ g_a\in G),$$

以及内积(不同表示的行矢量)

$$\langle\Phi_\rho^{(i)},\Psi_\mu^{(i)}\rangle \equiv X_{\rho\mu}^{ji},$$

则由 $\Psi_\rho^{(jr)} = \sum_{\rho}\Phi_\rho(x)X_{\rho\mu}^{(ir)}$，可得

$$\langle\Phi_\rho^{(i)},P_a\Psi_\mu^{(i)}\rangle = \sum_{\nu}\langle\Phi_\rho^{(i)},\Psi_\nu^{(i)}\rangle\Gamma^{(i)}(g_a)_{\nu\mu}$$

$$= \sum_{\nu} X^{ji}_{\rho\nu} \Gamma^{(i)}(g_a)_{\nu\mu}, \forall\ g_a \in G.$$

由内积的性质得

$$\begin{aligned}\langle \Phi^{(j)}_{\rho}, P_a \Psi^{(i)}_{\mu} \rangle &= \langle \Phi^{(j)}_{\rho}, P_a \Psi^{(i)}_{\mu} \rangle = \langle P_a^{-1} \Phi^{(j)}_{\rho}, \Psi^{(i)}_{\mu} \rangle \\ &= \sum_{\lambda} \Gamma^{(j)}(g_a^{-1})^{*}_{\lambda\nu} \langle \Phi^{(j)}_{\lambda}, \Psi^{(i)}_{\mu} \rangle = \sum_{\nu} X^{ji}_{\lambda\mu} \Gamma^{(i)}(g_a)_{\rho\lambda}.\end{aligned}$$

也就是说，

$$X^{ji} \Gamma^{(j)}(g_a) = \Gamma^{(i)}(g_a) X^{ji}, \forall\ g_a \in G.$$

由舒尔第二引理得

$$X^{ji} = \begin{cases} 0 & (j \neq i, \text{即不同表示}), \\ \lambda I & (j = i, \lambda \text{ 常数}). \end{cases}$$

§ 4.2 Wigner-Eckart 定理的应用

定义 4.2.1 若能级 E 对应的表示是不可约的，则简并($m > 1$)称为正则简并；若对应可约表示则称偶然简并.

设系统的哈密顿量为 $H = H_0 + H_1$，其中微扰 H_1 与 H_0 有相同对称性，即

$$[P_a, H_0] = 0, \quad [P_a, H_1] = 0.$$

设 $\{\Gamma^{(i)}(g_a)\}$ 为确定波函数 $\Psi^{(i)}_{\mu}(x)$ 的不可约表示，

$$P_a \Psi^{(i)}_{\mu}(x) = \sum_{\nu} \Psi^{(i)}_{\nu}(x) \Gamma^{(i)}(g_a)_{\nu\mu}, \qquad \forall\ g_a \in G,$$

且

$$\begin{aligned}P_a[H_1 \Psi^{(i)}_{\mu}(x)] &= H_1 P_a \Psi^{(i)}_{\mu}(x) \\ &= \sum_{\nu} [H_1 \Psi^{(i)}_{\nu}(x)] \Gamma^{(i)}(g_a)_{\nu\mu}.\end{aligned}$$

对于正则简并，能量一级微扰矩阵元

$$E^{(i)}_{\nu\mu} = \langle \Psi^{(i)}_{\nu}, H_1 \Psi^{(i)}_{\mu} \rangle = \delta_{\nu\mu} \Delta E,$$

其中

$$H_0 \Psi^{(i)}_{\mu}(x) = E \Psi^{(i)}_{\mu}(x), H_1 \Psi^{(i)}_{\mu}(x) = \Delta E \Psi^{(i)}_{\mu}(x).$$

也就是说，能级发生平移，但未分裂. 此种对称微扰不会消除正则简并.

对于偶然简并，属同一不可约表示的各行的波函数，能级有相同移动不会分裂. 但对属于两个不等价不可约表示的波函数，能级移动不相等，能级会发生分裂，简并会部分消除，直到变成正则简并. 一般有

$$\langle \Psi^{(i)}_{\mu}, H_1 \Psi^{(j)}_{\nu} \rangle = \delta_{\mu\nu} \delta_{ij} \Delta E.$$

例 4.2.1 二面体群 D_6 对苯分子能级的计算中的简化

图 4.1 为苯(C_6H_6) 分子结构图,其中每个碳原子的 4 个价电子,有 3 个 σ 电子紧紧束缚在碳原子上,其波函数主要分布在碳 — 碳与碳 — 氢的主键上. 另一个价电子即 π 电子绕苯环转动,主要垂直于环平面(图 4.2).

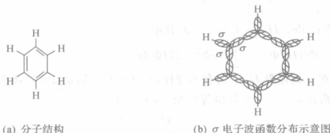


图 4.1　苯分子结构图

碳 $Z = 6$,K 壳层($n = 1, l = 0$) 有 2 个电子(填满),L 壳层($n = 2, l = 0, l = 1$) 有 8 个电子(4 个空着)

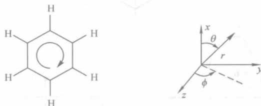


图 4.2　苯分子中局域化的 π 电子

设系统的哈密顿方程为 $H\Psi = E\Psi$,其中 $H = H_0 + H_1, H_0 = \dfrac{p_i^2}{2m}$ (p_i 与 m 为第 i 个电子的动量和质),$H_1 = -\sum_i \dfrac{Ze^2}{|r - r_i|}$ 表示电子与碳原子核的相互作用. 采用变分法解决此问题.

$$\delta E = \delta \frac{\Psi | H | \Psi}{\langle \Psi | \Psi \rangle} = 0.$$

其中 $\Psi(r)$ 表示内部 π 电子(p 波) 的近似波函数,

$$\Psi(r) = \sum_{i=1}^{6} a_i \Phi(r - r_i),$$

a_i 为待定函数,r_i 表示第 i 个碳原子的位置. 简记

$$\Phi_i = \Phi(r - r_i)(i = 1, 2 \cdots 6),$$

解本征值方程以确定 $\{a_i\}, i = 1, 2 \cdots 6$(令 $\Phi(r) = br\cos\theta e^{-ar}$, b 为常数),

$$(H_{ij})\begin{pmatrix}a_1\\a_2\\\vdots\\a_6\end{pmatrix}=E\begin{pmatrix}a_1\\a_2\\\vdots\\a_6\end{pmatrix}(i,j=1,2,\cdots,6),$$

或等价的久期方程 $\det|H_{ij}-E\delta_{ij}|=0$，其中

$$H_{ij}=(\Phi_i|H|\Phi_j)=\int d^3x\Phi_i^*(r)H\Phi_j(r).$$

注意到 H 在二面体群 D_6 下具有不变性，令 $a=C'_6$（转动 $2\pi/6$），b 为对 x 轴的反射操作（图 4.3），则有 $a^6=b^2=I$（恒等变换），$aba=b$.

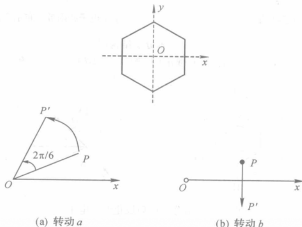


图 4.3　D_6 二面体对称操作

集合 $D_6=\{I,a,a^2,a^3,a^4,a^5,b,ba,ba^2,ba^3,ba^4,ba^5\}$，

阶 $g=12$，有 6 个类（$c=K=6$），（注意：$a^n=a^{-(6-n)},n\leqslant 5$）

$e_1=\{I\},n_1=1;e_2=\{a^3\},n_2=1;e_3=\{a,a^{-1}\},n_3=2;$

$e_4=\{a^2,a^{-2}\},n_4=2;e_5=\{a^3,a^{-3}\},n_5=2;$

$e_6=\{b,ba^2,a^2b\},n_6=3.$

由伯恩塞德定理 $g=\sum_{i=1}^{6}l_i^2=12$，有

$l_1=l_2=l_3=l_4=1,l_5=l_6=2.$

利用 Wigner-Eckart 定理，$\forall\ g_a\in D_6,g_a^{-1}H=Hg_a$，有

$\langle\Phi_\rho^{(i)}|H_1|\Phi_\sigma^{(j)}\rangle=\delta_{ij}\delta_{\rho\sigma}\langle i|H_1|i\rangle$，

其中 $\Phi_\rho^{(i)}$ 为群 D_6 的第 i 个不可约表示 $\{\Gamma_g^{(i)}\}$ 的相应表示空间的基，$\rho=1,2,\cdots,6$，

即

$$P_a \Phi_\rho^{(i)}(x) = \sum_{\sigma=1}^{6} \Phi_\sigma^{(i)}(x) \Gamma^{(i)}(g_a)_{\sigma\rho}.$$

$\Phi_\sigma^{(j)}$ 亦即 $\langle i|H_1|i\rangle$，为与表示 i 和 j（或者量子数 i 和 j）无关的约化矩阵元. 如此会将久期方程约化为几个独立小块，而每小块又相应更小的不可约表示矩阵.

换言之，苯分子能级按 D_6 的不可约表示分类，每个表示的维数相应于能级的简并度（不计偶然简并）.

先寻找 D_6 的生成元 a 与 b 的 6×6 表示矩阵 $\Gamma(a)$ 与 $\Gamma(b)$，再将它们约化，提出较低维的不可约表示分量.

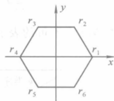


图 4.4

注意图 4.4 中 x 轴连接第一与第四个碳原子，与前图不同. 令 P_a 与 P_b 表示生成元 a 与 b 操作（r_i 为固定矢量）.

$$P_b\Phi_i(r) = P_b\Phi_i(r - r_i) = \Phi$$

$$P_a(r - r_i) = \Phi(P_a(r - P_a{}^{-1}r_i)) = \Phi(r - P_a{}^{-1}r_i)$$

$$P_{bi}(r - r_i) = P_b = P_b\Phi_i(r - r_i) = \Phi(r - r_i)P_b,$$

其中利用了对称关系

$$\Phi(P_a(r)) = \Phi(r).$$

对于近似波函数 $\Phi(r) = br\cos\theta e^{-ar}$ 具有更高的轴对称性.

$$P_b\Phi_i(r) = P_b\Phi_i(r - r_i) = \Phi(P_a(r - (r_i))$$

亦即 P_b 与 P_a 的作用使得

$$P_a: \Phi_1 \to \Phi_2 \to \Phi_3 \to \Phi_4 \to \Phi_5 \to \Phi_6 \to \Phi_1 \text{（轮换）},$$

$$P_b: \Phi_1 \to \Phi_1, \Phi_2 \leftarrow\to \Phi_6, \Phi_3 \leftarrow\to \Phi_5, \Phi_4 \leftarrow\to \Phi_4,$$

由

$$P_a\Phi_p = \sum_a \Phi_b \Gamma_{ap}(a)$$

写成矩阵形式

$$(\Phi_1\Phi_2\Phi_3\Phi_4\Phi_5\Phi_6)\begin{pmatrix} \Gamma(a)_{11} & \Gamma(a)_{12} & \cdots & \Gamma(a)_{16} \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ \Gamma(a)_{61} & \cdots & \cdots & \Gamma(a)_{66} \end{pmatrix} = \begin{pmatrix} \Phi_1 \\ \Phi_2 \\ \vdots \\ \Phi_6 \end{pmatrix}$$

易得 $\Gamma(a)$ 的显示表达式，同样可得 $\Gamma(b)$：

$$\Gamma(a) = \begin{pmatrix} & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \\ 1 & & & & & \end{pmatrix};\Gamma(b) = \begin{pmatrix} 1 & & & & & \\ & & & & & 1 \\ & & & & 1 & \\ & & & 1 & & \\ & & 1 & & & \\ & 1 & & & & \end{pmatrix}$$

现在约化这个表示，为此必须找到不可约表示的基．利用群 D_6 的特征标（表 4.1）(D_6 群为异常群，特征标均为实数）和约化公式

$$\Gamma(g_a) = \sum_{\oplus i=1}^{b} m_i \Gamma^{(i)}(g_a), \forall\ g_a \in G = D_6, \chi(g_a) = \sum_i m_i \chi_i(g_a)$$，其中 $\Gamma^{(i)}(g_a)$ 为 D_6 的第 i 个不可约表示，$m_i = \dfrac{1}{12}\sum_{k=1}^{6} n_k \chi_i^{(k)} \chi^{(k)}$，$k$ 为群元类序号．

表 4.1　群 D_6 的特征标表

k 类序号 / i 不可约表示	e_1 $n_1 = 1$	e_2 $n_2 = 1$	e_3 $n_3 = 2$	e_4 $n_4 = 2$	e_5 $n_5 = 3$	e_6 $n_6 = 3$
$\chi_1^{(k)}$	1	1	1	1	1	1
$\chi_2^{(k)}$	1	1	1	1	-1	-1
$\chi_3^{(k)}$	1	-1	-1	1	1	-1
$\chi_4^{(k)}$	1	-1	-1	1	-1	1
$\chi_5^{(k)}$	2	2	-1	-1	0	0
$\chi_6^{(k)}$	2	-2	1	-1	0	0

其中 E_1, E_4, E_5 和 E_6 为本征值，具体数值应由数值计算．

$$E_1 < E_4 < E_5 < E_6.$$

能级 E_1、E_6 有两个 π 电子，E_5 和 E_6 则有 4 个 π 电子．苯分子系统基态是 $2\Gamma_1 + 4\Gamma_6$ 态，激发态是 $2\Gamma_1 + 3\Gamma_6 + \Gamma_5$ 态．维一爱定理在原子核核谱的计算、量子力学中 K-G(Klein-Gordon) 系数的计算中还有广泛的应用．

问题 4.2

1. 完成 D_6 群特征标表的具体计算．

2. 证明由 $\Psi_\rho^{(jr)} = \sum_\rho \Phi_\rho(x) X_{\rho\mu}^{(ir)}$ 式定义的投影算符具有以下性质：

$$P_\mu^{(i)} P_\nu^{(j)} = \delta_{iu}\delta_{\mu\nu} P_\mu^{(i)} \qquad P^{(i)} P^{(j)} = \delta_{ij} P^{(i)}$$（正交性、等幂性），

$$\sum_i P^{(i)} = \sum_{i,\mu} P_\mu^{(i)} = I \text{（单位矩阵），（完备性）.}$$

§4.3　对称群的标准表示

这一节我们研究对称群 S_n 的群结构及各类表示，正则表示是有限群的忠实表示，其一般定义前面已经谈到，本节主要讨论对称群的正则表示.

1. 正则表示

给出映射　$f: P \to n \times nf(P)$ 矩阵.

矩阵中只有 n 个元素等于1，其余均为0；置换 P 的每一列确定 P 的一个非零矩阵元 $f(P)_{ij}$；其中的第一行数字为列脚标 j，第二行数字为行脚标 i. 置换对象的一种排列即视为行矢量.

例 4.3.1

$$P = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}^{(j)}_{(i)} \to f(P) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

$$(a_1 \quad a_2 \quad a_3 \quad a_4) \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = (a_4 \quad a_1 \quad a_3 \quad a_2).$$

显见 P 与 $f(P)$ 有一一对应的关系，效果完全相同.

一般规则：设有　$P_i = \begin{bmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$，

则 $f(P)$ 的矩阵元按上述规则，有

$$[f(P_i)]_{\alpha\beta} = \delta_{\alpha i_1}\delta_{1\beta} + \delta_{\alpha i_2}\delta_{2\beta} + \cdots + \delta_{\alpha i_n}\delta_{n\beta} (\alpha, \beta = 1, 2, \cdots, n).$$

容易验证集合 $\{f(P_\alpha) | \forall\, P_\alpha \in G\}$ 是群的一个忠实表示，常称其为正则表示. 正则表示的维数等于置换群 S_n 的阶 $n!$（即 S_n 的元素个数）.

由凯莱定理，任何有限群 G 都等价于在其群元集合上的置换群 $\{P(g_\alpha)\}$，其中

$$P(g_\alpha) = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_\alpha g_1 & g_\alpha g_2 & \cdots & g_\alpha g_n \end{bmatrix}.$$

应用上述规则，可得到正则矩阵的集合：$\{\Gamma^{reg}(g_\alpha)\}$，给出群 G 的正则表示. 这里的定义与前面的定义是完全等价的.

2. 维数定理

由于整数 n 的可能配分数等于 S_n 的不等价不可约表示的数目,故可以用配分作为 S_n 不可约表示的标记.尤其用 Young 图表示配分极其简易直观.

所谓 Young 图,就是对整数 n 按一种配分$[\lambda]=[\lambda_1,\lambda_2,\cdots,\lambda_K]$,将 n 个方格按如下规则排列起来的方格图,其中第 i 行的格子数为 $\lambda_i(1\leqslant i\leqslant K)$.由于分配的规定,$\lambda_{i+1}\leqslant\lambda_i$,因此 Young 图的下一行格子数不会超过上面各行的格子数.

例 4.3.2　配方[421]对应的 Young 图[图 4.5(a)]及其共轭 Young 图[图 4.5(b)].

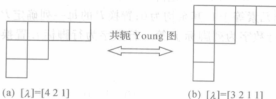


图 4.5

行列互换的 Young 图成为原 Young 图的共轭 Young 图,其配分成为共轭配分,可以证明共轭表示的特征标有关系 $\chi^{[\tilde{\lambda}]}=\chi^{[\lambda]}\cdot\chi^{[11\cdots1]}$.

对应 S_n 群的 Young 图,用 $1,2,\cdots,n$ 这 n 个整数填充 Young 图,使每一行的数字从左到右不减少,每一列的数字从上到下不减少,所得到的若干填满数字的,称为 Young 盘.Young 盘与 S_n 的不可约表示关系密切,有如下重要的维数定理.

维数定理　对称群 S_n 的配分$[\lambda]$所对应的的维数等于该配分 Young 图可以填充的 Young 盘的个数.

例 4.3.3　$S_3(g=3!=6)$共 3 个共轭类$(K=3)$,对应 3 种配分[3]、[2 1]和[1 1 1],代表 3 个不等价不可约表示,记为 $\Gamma^{[3]}$,$\Gamma^{[21]}$ 和 $\Gamma^{[111]}$.

由佰恩塞德定理有:$6=1^2+1^2+2^2$.其 Young 图和 Young 盘如图 4.6 所示.

可以证明,对应配分$[\lambda]=[\lambda_1,\lambda_2,\cdots,\lambda_k]$的 Young 图,总计 Young 盘数为

$$f(S_n:[\lambda])=\frac{n!}{m_1!m_2!\cdots,m_k!}\prod_{i<j}^{k}(m_i-m_j),$$

其中,$m_i=\lambda_i+K-i$,K 为 Young 图实际行数.

3. 对称群 S_n 的标准表示

显然 S_{n-1} 是 S_n 的子群,依此类推,得到置换群的子群约化链

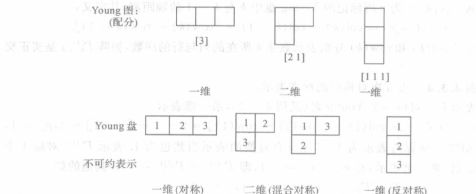


图 4.6

$$S_n \supset S_{n-1} \supset S_{n-2} \supset \cdots \supset S_2 \supset S_1.$$

另一方面，对于 S_n 的一个表示 A_n，从 A_n 中抽出与 S_{n-1} 对应的元素 A_{n-1}，则 A_{n-1} 也是 S_{n-1} 的元素，我们也可以得到表示的"子表示"链，

$$A_n \supset A_{n-1} \supset A_{n-2} \supset \cdots \supset A_2 \supset A_1.$$

它们的相应表示空间亦有如此链式结构. 但对于群来说，$A_{n-1}, A_{n-2}, \cdots, A_2, A_1$ 等不一定是不可约的. 所谓标准表示，就是通过基底变换，使 A_n 都是完全约化的形式，或 $A_{n-1}, A_{n-2}, \cdots, A_2, A_1$ 均成为相应子群的不可约表示.

$\forall\ P_i \in S_n$，设将 P 约化为一系列对换乘积，再利用恒等式：

$$(ab\cdots de\cdots h) = (ab\cdots d)(de\cdots h),\ (ab) = (ca)(cb)(ca),$$

总可以把置换的乘积改写为相邻对象的对换算符 $P_{k-1,k}(k = 2, 3, \cdots, n)$ 的乘积. 只要能给出 $P_{k-1,k}$ 的表示矩阵，就可以用矩阵相乘，得到任何置换的表示. $\{P_{k-1,k}\}$ 是 S_n 群的生成元. 令 $\{U_{k-1,k}^{(\lambda)} | k = 2, 3, \cdots, n\}$ 标记对应配分 $[\lambda]$ 的不可约表示的相邻对换算子的标准表示矩阵（共 $n-1$ 个）. 其矩阵元 $(\Gamma_{k-1,k}^{(\lambda)})_{rs} \equiv \langle [\lambda] r | P_{k-1,k} | [\lambda] s \rangle$，其中 r 和 s 为 $[\lambda]$Young 图中不同 Young 盘的标记. 对于 r 和 s 标记的 Young 盘，矩阵元 $(U_{k-1,k}^{(\lambda)})_{rs}$ 由下式确定：

$$(\Gamma_{k-1,k}^{(\lambda)})_{rs} = \begin{cases} \underset{\text{对角元}}{(\Gamma_{k-1,k}^{(\lambda)})_{rs}} = \langle [\lambda] r | P_{k-1,k} | [\lambda]_s \rangle \\ \qquad = [\rho_{k-1,k}([\lambda] r)]^{-1} \\ \underset{(r \neq s)\text{非对角元}}{(\Gamma_{k-1,k}^{(\lambda)})_{rs}} = \begin{cases} [1 - (\rho_{k-1,k}([\lambda] r))^{-2}]^{\frac{1}{2}}, \\ \quad \text{当 } k \text{ 与 } k-1 \text{ 互换时,} \\ \quad \text{Young 盘 } r \text{ 与 } s \text{ 亦互换,} \\ 0, \quad \text{其他,} \end{cases} \end{cases}$$

其中 $\rho_{k-1,k}([\lambda]r)$ 为 r 所标记的 Young 盘中 k 与 $k-1$ 的轴距离，其定义：

$$\rho_{k-1,k}([\lambda]r)=\text{col}(k)-\text{col}(k-1)-[\text{row}(k)-\text{row}(k-1)].$$

符号 col(k) 和 row(k) 分别表示数字 k 所在的列与行的序数，矩阵 $\Gamma_{k-1,k}^{[\lambda]}$ 是实正交的.

例 4.3.4　求 3 次对称群的标准表示.

表示 $\Gamma^{[3]}$ 对应一个 Young 盘(见例 4.3.3)，系一维表示

$\rho_{12}=\text{col}(2)-\text{col}(1)-[\text{row}(2)-\text{row}(1)]=2-1-[1-1]=1,\rho_{23}=1,$ 相应相邻对换算符表示为 1. 其他所有置换的表示当然也为 1. 表示 $\Gamma^{[111]}$ 对应 1 个 Young 盘，系一维表示，有 $\rho_{12}=\rho_{23}=-1$，即 $\Gamma_{1,2}^{[111]}=\Gamma_{2,3}^{[111]}=-1$. 其他的如

$$\Gamma_{13}^{[111]}=\Gamma_{23}^{[111]}\Gamma_{21}^{[111]}\times\Gamma_{23}^{[111]}=(-1)^3=-1,$$

$$AS\Gamma_{132}^{[111]}=\Gamma_{13}^{[111]}\Gamma_{32}^{[111]}=(-1)^3\cdot(-1)=1.$$

即奇置换为 -1，偶置换为 1.

表示 $\Gamma^{[21]}$ 对应两个 Young 盘，记为 1 和 2$(r=1,2)$，系二维表示. 对于 Young 盘 1，当数字 $1\leftrightarrow2$ 时，$\Gamma_{12}^{[21]}$ 的

1	2
3	

$1\overset{\neq}{\longleftrightarrow}2$

2	1
3	

(不标准 Young 盘) ⟵⟶ 非对角元素为 0 .

对角元素

$$(\Gamma_{12}^{[21]})_{11}=\langle[21]1|P_{1,2}|[21]1\rangle_{11}=\rho_{12}^{-1}([21]1)=1,$$

$$(\Gamma_{12}^{[21]})_{22}=\langle[21]2|P_{1,2}|[21]2\rangle=\rho_{12}^{-1}([21]2)=-1,$$

即

$$\Gamma_{12}^{[21]}=\begin{bmatrix}1&0\\0&-1\end{bmatrix}.$$

再考虑表示矩阵 $\Gamma_{23}^{[21]}$，注意到 Young 盘 2$(r=2)$，当 $2\leftrightarrow3$ 时，

1	3
2	

$2\longleftrightarrow3$ $(r=2)$

1	2
3	

⟺

1	2
3	

$(r=1)$，

亦即此时矩阵的非对角矩阵元不为零，有

$$(\Gamma_{2,3}^{[21]})_{12}=\langle[21]1|P_{2,3}|[21]2\rangle=(1-(\rho_{23}([21]2)^{-2})^{1/2}$$

$$=(1-(\frac{1}{2})^2)^{\frac{1}{2}}=\frac{\sqrt{3}}{2}=(\Gamma_{23}^{[21]})_{21}.$$

至于对角元 $(\Gamma_{23}^{[21]})_{11}=\langle[21]1|P_{2,3}|[21]1\rangle=\rho_{23}([21]1)^{-1}=-1/2,$

$$(\Gamma_{23}^{[21]})_{22}=\rho_{23}([21]2)^{-1}=\frac{1}{2},$$

即 $$\Gamma^{[21]}_{23} = \frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ \sqrt{3} & -1 \end{bmatrix}.$$

其余表示矩阵可以同样得到，见表 4.2.

表 4.2　S_3 群的标准表示

群元 \ 表示	$\Gamma^{[3]}$	$\Gamma^{[21]}$	$\Gamma^{[111]}$
E	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1
(123)	1	$\frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}$	1
(23)	1	$\frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ \sqrt{3} & 1 \end{bmatrix}$	-1
(13)	1	$\frac{1}{2}\begin{bmatrix} -1 & -\sqrt{3} \\ -\sqrt{3} & 1 \end{bmatrix}$	-1
(132)	1	$\frac{1}{2}\begin{bmatrix} -1 & \sqrt{3} \\ -\sqrt{3} & -1 \end{bmatrix}$	$+1$
(12)	1	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	-1

问题 4.3

1. 对称群 S_n 中任一元素分解为对换乘积时，对换总数的奇偶性不变.

[提示：构造范德蒙(Vandermonde)行列式.

$$D(x_1,x_2,\cdots,x_n) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \cdots & \cdots & \cdots & \\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{i>j}(x_i - x_j),$$

在任何对换作用下，$D(x_1,x_2,\cdots,x_n)$ 改变符号. $\forall\, g_a \in S_n$，且 g_a 分解成 k 个对换，则 $g_a D = (-1)^k D$，因子 $(-1)^k$ 与分解的方式无关.]

2. 设 $\forall\, g_a \in S_n$，$a_i^{(j)}(j = 1,\cdots,n; i = 1,\cdots,j)$ 取 $1,2\cdots,n$，若有

$x \in L_G, x = (a_1)^{a_1}(a_1^{(2)},a_2^{(2)})^{a_2}\cdots(a_1^{(n)},a_2^{(n)},\cdots,a_n^{(n)})^{a_n}$,

则

$$g_a^{-1}\chi g_a = (b_1)^{a_1}(b_1^{(2)},b_2^{(2)})^{a_2}\cdots(b_1^{(n)},b_2^{(n)},\cdots,b_n^{(n)})^{a_n},$$

其中 $b_i^{(j)}(i=1,\cdots,j;j=1,\cdots,n)$ 取 $1,2\cdots,n$,亦称共轭变换不改变结构$(1^{a_1}2^{a_2}\cdots n^{a_n})$,$S_n$ 群共轭类可以用配分 $n=\alpha_1+2\alpha_2+\cdots+n\alpha_n$ 表征.

[提示:$(i',j)^{-1}=(j,i)=(i,j)$,故 $(i,j)^{-1}(a_1,a_2,\cdots,a_n)(i,j)=(a'_1,a'_2,\cdots,a'_n)$,轮换长度不变.此外,$\forall\ g_a\in S_n$,总可以分解为

$$g_a=(b_1,b'_1)(b_2,b'_2)\cdots(b_p,b'_p),$$

$$g_a^{-1}=(b_p,b'_p)^{-1}(b_{p-1},b'_{p-1})^{-1}\cdots(b_1,b'_1)^{-1},$$

故 $g_a^{-1}(a_1,a_2,\cdots,a_k)g_a=(a'_1,a'_2,\cdots,a'_k)$,如此等等.]

3. 试证明由 $[f(P_i)]_{\alpha\beta}=\delta_{\alpha i_1}\delta_{1\beta}+\delta_{\alpha i_2}\delta_{2\beta}+\cdots+\delta_{\alpha i_n}\cdot\delta_{n\beta}$ 式给出的矩阵集合 $\{f(P_a)\}$,是群 S_n 的一个忠实表示.

[提示:$[f(P_i)f(P_j)]_{\alpha\beta}=\sum_r[f(P_i)]_{\alpha\gamma}[f(P_i)]_{\gamma\beta}=\sum_r(\delta_{\alpha i_1}\delta_{1\gamma}+\cdots+\delta_{\alpha i_n}\delta_{n\gamma})\cdot(\delta_{\gamma_1}\delta_{k_1\beta}+\cdots+\delta_{\gamma_n}\delta_{k_n\beta})=\delta_{\alpha i_1}\delta_{k_1\beta}+\cdots+\delta_{\alpha i_n}\delta_{k_n\beta}=[f(P_iP_j)]_{\alpha\beta}$,其中用到

$$P_i=\begin{bmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{bmatrix},P_j=\begin{bmatrix}1 & 2 & \cdots & n\\ j_1 & j_2 & \cdots & j_n\end{bmatrix}=\begin{bmatrix}k_1 & k_2 & \cdots & k_n\\ 1 & 2 & \cdots & n\end{bmatrix},$$

$$P_iP_j=\begin{bmatrix}k_1 & k_2 & \cdots & k_n\\ i_1 & i_2 & \cdots & i_n\end{bmatrix}.]$$

4. 对于 S_n 中配分 $[\lambda]=[31]$,画出相应的 Young 图和 Young 盘,指出对应不可约表示的维数,并给出相应的标准表示 $\Gamma_{S_4}^{[31]}$.

§4.4　对称群表示的约化

对称群的可约表示,当然可以用标准的特征标方法进行约化.找到标准表示,意味着找到了对称群 S_n 的全部不等价不可约表示,但是对于对称群的表示的约化却有特别简易可行的特殊办法.本节主要讨论对称群表示的约化问题.

1. 对称群 S_n 的分支律

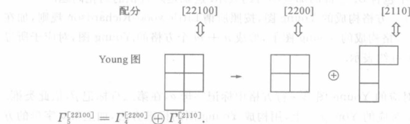
对称群 S_n 的不可约表示,一般说来,对于 $S_m(m<n)$ 群是可约表示.我们希望了解,在对称群 S_n 的不可约表示 $\{\Gamma_n^{[\lambda]}\}$ 中包含对称群 S_m 的哪些不可约表示.为此只需研究包含 S_{n-1} 群的不可约表示就可以了.然后采取逐步递推的办法,来解决问题.

将对应对称群 S_n 不可约表示 $\{\Gamma_n^{[\lambda]}\}$ 的 n 个格子构成的 Young 图,以不破坏 Young 图规则为原则,用各种可能的方式去掉 1 个小方格,所得到的 $(n-1)$ 个方格构成的

Young 图,对应着在$\{\Gamma_n^{[\lambda]}\}$中所包含的所有对称群 S_{n-1} 可约表示$\{\Gamma_n^{[\lambda']}\}$…,这就是所谓的分支律,可表述为:

$$\Gamma_n^{[\lambda_1\lambda_2\cdots\lambda_n]} = \sum_{\oplus\lambda_1\geqslant\cdots\geqslant\lambda_{i-1}\geqslant\cdots\geqslant\lambda_n} \Gamma_{n-1}^{[\lambda_1\cdots\lambda_i^{-1}\cdots\lambda_n]}.$$

例 4.4.1　将 S_5 的不可约表示$\{\Gamma_5^{[22100]}\}$约化为 S_4 的不可约表示$\{\Gamma_4^{[\lambda]}\}$,



$$\Gamma_5^{[22100]} = \Gamma_4^{[2200]} \oplus \Gamma_4^{[2110]}.$$

例 4.4.2　$\Gamma_7^{[3221]} = \Gamma_6^{[332]} \oplus \Gamma_6^{[3211]} \oplus \Gamma_6^{[2211]}$.

S_n 群不可约的两个表示的直积称为内积,也是 S_n 的一个表示. 其约化用 Young 图很方便.

例 4.4.3　$SU(3)$ 群中的内积.

若用 1 个方格代表 $SU(3)$ 的一个基础表示的基矢,数字 1,2,3… 有五种填充方法(Young 盘),故基础表示维数为 3. 两夸克态可表示为

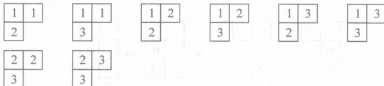
□ ⊗ □ = □□ (反对称) ⊕ 日 (对称)

其中□□用 1,2,3 填充可得 6 个 Young 盘(6 维表示),置二格图则对应 3 个 Young 盘(3 维表示).

如果 3 个夸克构成重子,则用 Young 图表示为

□ ⊗ □ ⊗ □ = 田 ⊕ □□□

此时注意,有补充规则,凡三格一列应删去,则右边第一图对应 8 个 Young 盘,即相应 8 维表示:



即是夸克模型中重子八重态("八正道"一词亦由此而来). 右边第二图,对应 1 个 Young 盘,是全对称单态.

可见，求内积实质上也是利用分支律，不过是反过来应用罢了.

2. S_n 与 S_m 群表示的外直积

所谓外直积就是 S_n 的不可约表示 $\Gamma_n^{[\lambda]}$ 与 S_m 的不可约表示 $\Gamma_m^{[\mu]}$ 的直积. 我们的目的在于探求外直积中包含 S_{n+m} 群的那些不可约表示. 这就是外直积的约化问题.

将$[\lambda]$对应 n 个方格构成的 Young 图，按照所谓 Littlewood-Richardson 规则，加在$[\mu]$对应的 m 个方格构成的 Young 图上，形成 $n+m$ 个方格的 Young 图，对应于所寻找的 S_{n+m} 群的不可约表示.

里氏规则是：

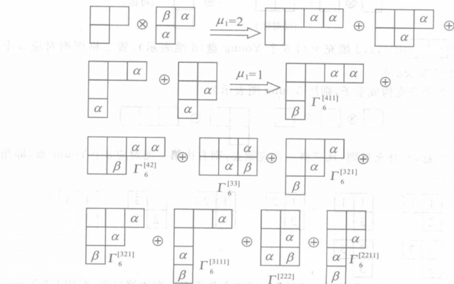
(1) 在$[\mu]$对应的 Young 图第一行方格中标记字母 α，在第二行标记 β，依此类推.

(2) 在$[\lambda]$所对应的 Young 图上，用构成 Young 图的标准方法，加上带 α 字母的方格(μ_1 个). 添加附加条件有：在同一列不允许有两个带 α 的方格出现.

(3) 用(2)所叙述方法，再在$[\lambda]$Young 图上添加带 β 的格子(有 μ_2 个). 但注意从右上角开始，从上到下逐行从右到左阅读，在任何时候，保证 β 格子所出现的次数不超过 α 格子出现的次数.

(4) 用同样方法添加带 γ 的格子，如此类推.

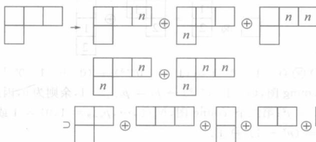
例 4.4.4　用里氏规则计算 $\Gamma_3^{[21]}\otimes\Gamma_3^{[21]}$.



$$S\Gamma_3^{[21]} \otimes \Gamma_3^{[21]} = \Gamma_6^{[42]} \oplus \Gamma_6^{[33]} \oplus \Gamma_6^{[411]} \oplus \Gamma_6^{[321]} \oplus \Gamma_6^{[321]} \oplus \Gamma_6^{[3111]} \oplus \Gamma_6^{[222]} \oplus \Gamma_6^{[2211]}.$$

例 4.4.5　$SU(n)$ 群约化为 $SU(n-1)$ 的规则.

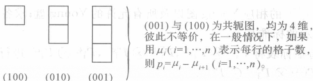
从表示的对应的标准 Young 图中用一切不破坏 Young 图规则的办法在格子上标记 n，然后去掉带 n 的方格，余下的 Young 图对应 $SU(n-1)$ 的不可约表示. 例如，



当 $n=4$ 的维数依次为 20206 维、10 和 4 维.

例 4.4.6　$SU(n)$ 群的维度公式.

$SU(n)$ 群的 $n-1$ 基础表示用 $n-1$ 个单列 Young 图表示，每行格子数为 $i(i=1,2,\cdots,n-1)$，用 $n-1$ 个整数表征，如 $SU(4)$，



一般有递推公式，$SU(n-1)$ 群的维数

$$\begin{aligned} N_{n+1} &= (p_1, p_2, \cdots, p_n) \\ &= \frac{1}{n!\cdots 2!}(p_1+1)(p_1+p_2+2)+\cdots+(p_1+p_2+\cdots p_n+n) \\ &\quad \cdot (p_2+1)(p_2+p_3+2)\cdots(p_2+\cdots+p_n+n-1)\cdots(p_n+1), \end{aligned}$$

或

$$N_{n+1}(p_1,p_2,\cdots,p_n) = \frac{(p_n+1)(p_n+p_{n-1}+2)\cdots(p_n+p_{n-1}+\cdots+p_1+n)}{n!}.$$

特别地，对于 $SU(2)$ 有

$$N_2(p) = p+1,$$

对于 $SU(3)$ 和 $SU(4)$ 有

$$N_3(p_1p_2) = \frac{1}{2}(p_1+1)(p_1+p_2+2)(p_2+1),$$

$$N_4(p_1p_2p_3) = \frac{1}{2!3!}(p_1+1)(p_1+p_2+2)\cdot(p_1+p_2+p_3+3)$$
$$\cdot(p_2+1)(p_2+p_3+2)(p_3+1).$$

对于 $SU(n)$ 第一个与第二个基础表示的直积

$$\boxed{} \otimes \begin{array}{|c|}\hline 1 \\ \hline 2 \\ \hline \end{array} = \begin{array}{|c|c|}\hline & 1 \\ \hline 2 \\ \cline{1-1} \end{array} \oplus \begin{array}{|c|}\hline \\ \hline 1 \\ \hline 2 \\ \hline \end{array}$$

$$(1\quad 0^{n-2})\otimes(0\quad 1\quad 0^{n-3}) = (1\quad 1\quad 0^{n-3}) + (0\quad 0\quad 1\quad 0^{n-4}).$$

右边第一个 Young 图，$(1\quad 1\quad 0^{n-3}) \rightarrow p_1 = p_{n-1} = 1$，余则为 0，因此 $N_n(p_1=1, 0,\cdots,0,p_{n-1}=1) = n^2$；第二个 Young 图，$N_n(0,\cdots,p_{n-2}=1,0) = 1$ 或表为数码字：

$$\textcircled{n}\otimes\textcircled{\bar{n}} = (n^2-1)\oplus\textcircled{1}.$$

对于 $SU(3)$，

$$\textcircled{3}\otimes\textcircled{\bar{3}} = \textcircled{8}\oplus\textcircled{1}.$$

问题 4.4

1. 用 S_3 群的表示 $\Gamma_6^{[321]}$ 将 $S_3\otimes S_3$ 的不可约表示约化，并检验表示维数.

2. 写出表示 $\Gamma_5^{[32]}$ 的相应 Young 图以及所有允许的 Young 盘；求各共轭类的特征量以及此不可约表示的标准基.

3. 利用 S_4 特征标表将 $\Gamma_4^{[4]}\otimes\Gamma_4^{[31]}$，$\Gamma_4^{[31]}\otimes\Gamma_4^{[31]}$，$\Gamma_4^{[4]}\otimes\Gamma_4^{[22]}$ 进行直积分解.

4. 求 S_3 的 $\Gamma_3^{[21]}\otimes\Gamma_3^{[21]}\otimes\Gamma_3^{[21]}$.

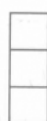
5. 给出 $SU(6)$ 群下述 Young 图的 $\{p_1,p_2,p_3,p_4,p_5\}$ 表示，并计算其相应维度.



(a)



(b)



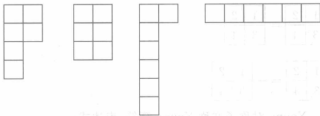
(c)

Young 图(a)、(b)、(c) 在 $SU(3)$ 群和 $SU(2)$ 群相应表示的维度是多少.

6. 试根据表示的对称性，分析并指出上题各 Young 图对应的 $SU(6)$ 多重态，即表示维度）所包含的 $SU(3)$ 和 $SU(2)$ 多重态.

7. 在 $SU(6)$ 中，作直积表示 $\Gamma_6^{[30^5]}\otimes\Gamma_6^{[21^4]}$，写出相应 Young 图算式.

8. 在 $SU(6)$ 群中，下列 Young 图分别表示 $SU(6)$ 群的多少重态？



§ 4.5　Young 对称子及应用

对称群 S_n 的基矢当然也可以用一般有限群中构造基矢的方法求得，但实际上用所谓的 Young 对称子的办法却更有效、更方便. 同样的方法，可以推广到 $SU(n)$、$O(n)$、$SO(n)$ 等经典群中。在物理学中，可用同样的方法解决多粒子体系波函数的对称化问题.

设用 p 表示只改变列，而不改变行的置换；反之，q 则表示只改变行，而不改变列的置换，令 $\forall\ p_i \in S_n, \forall\ q_j \in S_n$，则集合$\begin{array}{|c|c|}\hline 1 & 2 \\ \hline & 4 \\ \hline \end{array}$，

$$a[f] = \sum_i p_i, b[f] = \sum_j \delta_j q_j,$$

其中，当 q_j 为偶置换时，$\delta_j = 1$；当 q_j 为奇置换时，$\delta_j = -1$，f_i 表示第 i 行格子数. 分别构成群空间中的子代数.

例 4.5.1　S_4；$f_1 = f_2 = 2, f_3 = f_4 = 0$.

$\{p_i\}$：$E, (1,2), (3,4), (1,2), (3,4)$.

其中如$(1,2),(3,4)\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 4 & 3 \\ \hline \end{array}$，

$\{q_i\}$：$E, (1,3), (2,4), (1,3), (2,4)$.

其中如$(1,3),(2,4)\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 3 & 4 \\ \hline 1 & 2 \\ \hline \end{array}$，

$$a[f] = E + (1,2) + (3,4) + (1,2)(3,4),$$
$$b[f] = E - (1,3) - (2,4) + (1,3)(2,4).$$

显然，对于此图，a 与 b 分别为对称算符与反对称算符.

容易验证

$$a[f]\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline\end{array}=\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline\end{array}$$

$$b[f]\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline\end{array}=-\begin{array}{|c|c|}\hline 1&2\\\hline 3&4\\\hline\end{array}$$

定义 4.5.1 Young 对称子亦称 Young 算符，表达式：

$$c[f]=\sum_{i,j}\delta q_j p_i.$$

对于例 4.5.1，此式右边有 19 项，

$$\begin{aligned}c[f]=&E+(1,2)+(3,4)+(1,2)(3,4)-(1,3)-(2,4)+(1,3)(2,4)\\&-(1,3)-(2,4)+(1,3)(2,4)-(1,3)(1,2)\\&-(1,3)(3,4)-(1,3)(1,2)(3,4)-(2,4)(1,2)-(2,4)(3,4)\\&-(2,4)(1,2)(3,4)+(1,3)(2,4)(1,2)\\&+(1,3)(2,4)(3,4)+(1,3)(2,4)(1,2)(3,4).\end{aligned}$$

根据 Young 对称子，可以定义 S_n 群的不可约表示空间的投影算符（或原始等幂元）：

$$P_{[f]}=\frac{d[f]}{n!}c[f],$$

其中 $d[f]$ 为相应 Young 图维数，它具有下列性质：

(1) $P_{[f]}\cdot P_{[f]}=P_{[f]}$.
$$\begin{array}{|c|c|}\hline 1&2\\\hline 3&\\\cline{1-1}\end{array}$$

(2) 原始性：

若 $P_{[f]}=P_{[1]}+P_{[2]}$，且 $P_{[1]}P_{[1]}=P_{[1]}$，

$P_{[2]}P_{[2]}=P_{[2]}$，$P_{[1]}P_{[2]}=P_{[2]}P_{[1]}=0$.

则 $P_{[1]}=0$ 或 $P_{[2]}=0$.

每一个 Young 图$[f]$，对应一个原始等幂元. 所有 Young 图对应的原始等幂元彼此相互独立，构成一组完备的集合.

例 4.5.2 对称群 S_3 的 Young 对称子与原始等幂元.

Young 对称子：$c[f]=c[210]=\sum_{i,j}\delta_j q_j p_i$.

其中 $a[210]=E+(1,2)$，$b[210]=E-(1,3)$.

$$c[210]=\sum_{i,j=1}^{2}\delta_j q_j p_i=I+(1,2)-(1,3)-(1,3)(1,2)$$

$$= I + (1,2) - (1,3) - (1,2,3).$$

原始等幂元

$$P_{[210]} = \frac{d[f]}{3!}c[210] = \frac{2}{3\times 2\times 1}c[210] = \frac{1}{3}c[210].$$

为了构造相应的幺正表示,令

$$\Phi_{\mu\nu\lambda} = \xi_\mu(1)\xi_\nu(2)\xi_\lambda(3)$$

为粒子1、2、3三个波函数的乘积,$\mu,\nu,\lambda = 1,2,3$,它们是三阶张量.易得

$$\begin{aligned}c[210]\Phi_{\mu\nu\lambda} &= [\xi_\mu(1)\xi_\nu(2) + \xi_\nu(1)\xi_\mu(2)]\xi_\lambda(3)\\ &\quad - [\xi_\lambda(1)\xi_\nu(2)\xi_\mu(3) + \xi_\lambda(1)\xi_\mu(2)\xi_\nu(3)]\\ &= \Phi_{\mu\nu\lambda} + \Phi_{\nu\mu\lambda} - \Phi_{\lambda\nu\mu} - \Phi_{\lambda\mu\nu} \equiv \Psi_{\mu\nu\lambda}.\end{aligned}$$

形式上记为

μ	ν
λ	

.

即对脚标 μ、ν 是对称化的,对 μ 与 λ 是反对称的,亦即

(1)$\Psi_{\mu\nu\lambda} = \Psi_{\nu\mu\lambda}$;

(2)$\Psi_{\mu\nu\lambda} + \Psi_{\nu\mu\lambda} + \Psi_{\lambda\nu\mu} = 0$

(消除全对称部分 $\boxed{\mu\ \nu\ \lambda}$ 的条件,即单态).由于

$$(1,2)\Psi_{\mu\nu\lambda} \equiv \xi_{\mu\nu\lambda} \Rightarrow (1,2) = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

即

$$(1,2)\xi_{\mu\nu\lambda} = \Psi_{\mu\nu\lambda},$$

$$\left.\begin{aligned}(1,3)\Psi_{\mu\nu\lambda} &= -\Psi_{\mu\nu\lambda}\\ (1,3)\Psi_{\mu\nu\lambda} &= \xi_{\mu\nu\lambda} - \Psi_{\mu\nu\lambda}\end{aligned}\right\} \Rightarrow (1,3) = \begin{pmatrix}-1 & 1\\ 0 & 1\end{pmatrix},$$

其中 $\xi_{\mu\nu\lambda} \equiv \Phi_{\nu\mu\lambda} + \Phi_{\mu\nu\lambda} - \Phi_{\nu\lambda\mu} - \Phi_{\mu\lambda\nu}$,

$$\left.\begin{aligned}(2,3)\Psi_{\mu\nu\lambda} &= \Psi_{\mu\nu\lambda} - \xi_{\mu\nu\lambda}\\ (2,3)\xi_{\mu\nu\lambda} &= -\xi_{\mu\nu\lambda}\end{aligned}\right\} \Rightarrow (2,3) = \begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}.$$

S_n 的正交基矢及幺正表示.

继续讨论例4.5.1,现将表示幺正化,就是找到在 S_3 变换下使二次型

$$f(\Psi,\xi) = \alpha\Psi^2 + \beta\Psi\xi + \lambda\xi^2$$

保持不变的表示.

由于 $(1,2)f(\Psi,\xi) = f(\Psi,\xi)((1,2)\Psi = \xi)$,

即

$$\gamma\Psi^2 + \beta\Psi\xi + \alpha\xi^2 = \alpha\Psi^2 + \beta\Psi\xi + \gamma\xi^2 \Rightarrow \alpha = \gamma.$$

也由于$(1,3)\Psi=\Psi-\xi$，$(1,3)f(\Psi,\xi)=f(\Psi,\xi)$，即

$$\alpha\Psi^2+\beta(-\Psi)(\xi-\Psi)+\gamma(\xi-\Psi)^2=\alpha\Psi^2+\beta\Psi\xi+\gamma\xi^2\Rightarrow\alpha+\beta=0,$$

即$f(\Psi,\xi)=\alpha\Psi^2+\alpha\Psi+\alpha\xi^2=\alpha(\Psi^2-\Psi\xi+\xi^2)$，在$S_3$置换下保持不变. 注意到，

$$2(\Psi^2+\xi^2-\Psi\xi)=\frac{3}{2}(\Psi-\xi)^2+\frac{1}{2}(\Psi+\xi)^2=(\Phi^{(1)}i)^2+(\Phi^{(2)}j)^2,$$

其中单位矢量$i\cdot j=0$，$\Phi^{(1)}=\sqrt{\frac{1}{2}}(\Psi-\xi)$与$\Phi^{(2)}=\sqrt{\frac{1}{2}}(\Psi+\xi)$为正交矢量.

由于

$$\left.\begin{aligned}(1,2)\Phi^{(1)}&=\Phi^{(1)}\\(1,2)\Phi^{(2)}&=-\Phi^{(2)}\end{aligned}\right\}\Rightarrow(1,2)=\begin{pmatrix}1&0\\0&-1\end{pmatrix},$$

$$\left.\begin{aligned}(1,3)\Phi^{(1)}&=-\frac{1}{2}\Phi^{(1)}-\frac{\sqrt{3}}{2}\Phi^{(2)}\\(1,3)\Phi^{(2)}&=-\frac{\sqrt{3}}{2}\Phi^{(1)}+\frac{1}{2}\Phi^{(2)}\end{aligned}\right\}\Rightarrow(1,3)=\begin{pmatrix}-\frac{1}{2}&-\frac{\sqrt{3}}{2}\\-\frac{\sqrt{3}}{2}&\frac{1}{2}\end{pmatrix},$$

$$\left.\begin{aligned}(2,3)\Phi^{(1)}&=-\frac{1}{2}\Phi^{(1)}+\frac{\sqrt{3}}{2}\Phi^{(2)}\\(2,3)\Phi^{(2)}&=-\frac{\sqrt{3}}{2}\Phi^{(1)}+\frac{1}{2}\Phi^{(2)}\end{aligned}\right\}\Rightarrow(2,3)=\begin{pmatrix}-\frac{1}{2}&\frac{\sqrt{3}}{2}\\\frac{\sqrt{3}}{2}&\frac{1}{2}\end{pmatrix}.$$

这正好是我们早先求得的S_3的标准表示.

为方便以后应用，我们再介绍 Young 对称子的一般性质与原始等幂元的正交化一般方法.

Young 对称子可以视为对称群代数中的矢量，一般可表为

$$c[f]=\sum_{\forall g_a\in S_n}F(g_a)g_a=\sum\delta_q qp,$$

其中系数$F(g_a)=0,\pm1$，当组合置换不能表为q_jp_i形式时，$F(g_a)=0$. 其实$F(g_a)$即δ_j.

根据$\{p_i\}$与$\{q_j\}$的定义，显然有

$$pa[f]=a[f]p=a[f].$$

注 意$a[f]$并不属于S_n，它等价于先取 Young 图$[f]$中每行的所有置换变换加起来，然后再将这些和式相加(横向置换)：

$$a[f]=\sum p=\sum(\prod_i p_i)=\prod(\sum p_i),$$

其中p表示 Young 图中第i行数字间的任意置换$p=\prod_i p_i$，即各行p_i的乘积. 同样，

$$b[f]=\sum\delta_q p=\sum(\prod_k\delta_{q_k}q_k)=\prod_k(\sum\delta_{q_k}\cdot q_k).$$

又有

$$qb[f] = b[f]q = \delta_q Q.$$

这样就得到 Young 对称子的重要性质：

$$c[f] = pc[f] = \delta_q c[f] = \delta_q pc[f]q,$$

进而可得组合系数

$$F(g_a) = F(pg_a) = \delta_q F(g_a q) = \delta_q F(pq),$$

尤其是若 $c[f]$ 中包含的置换 pq，有

$$1 = F(E) = F(p) = \delta_q F(q) = \delta_q F(pq),$$

一般说来，一个 Young 图如果可以对应 f_i 个 Young 盘，则亦对应 f_i 个正则 Young 对称子 $c^{(i)}_{[f]}$，它们可将由 S_n 所负载的 n!个函数基.

$$\forall\ p_i \in S_n, \varphi_i(1,2,\cdots,n) = p_i\varphi(1,2,\cdots,n) \quad (i = 1,2,\cdots,f_i),$$

$$\sum_{i=1}^{n} f_i = n!.$$

其中的 f_i 个函数按标准 Young 盘的混合对称化：

$$c^{(i)}[f]\varphi_i(1,2,\cdots,n) = \Psi_i(1,2,\cdots,n) \qquad (i = 1,2,\cdots,f_i),$$

f_i 个函数$\{\Psi_i\}$将构成 S_n 的一个不变子空间，负载 S_n 的不可约表示$[f]$. 与标准基比较，有寻找方便的优点. 对于每一个不可约表示，对应一个 Young 图，只要找到所有 Young 图，就可利用 Young 对称子得到 Young 氏基. 但缺点是非幺正的，而标准基却是幺正的.

利用 Young 对称子，构造正交的原始等幂元就是为了解决 Young 氏基的上述缺点. f_i 个互相正交的原始等幂元 $e_i(i = 1,2,\cdots,f_i)$ 是

$$e_i e_j = \delta_{ij} e_i \qquad (i,j = 1,2,\cdots,f_i),$$

其中 $e_i = c^{(i)}y^{(i)}$. 可以证明 $y^{(i)}$ 定义如下：

$$y^{(i)} = E - \sum_{j=i+1}^{f_i} p_{ij}y^{(j)}, \quad yf_i = E, \quad i \leqslant f_i,$$

相应构造的$\{e_i\}$满足正交条件，其中第二项是下列形式之和：

$$(-1)^m p_{ik}p_{kl}p_{lt}\cdots, i < k < l < t < \cdots,$$

m 为所包含的 p 因子个数.

所谓 Young 对称子的正交性系指 $C' \cdot C = 0$.

其中并不具备相互性，即上式并不表明 $C' \cdot C = 0$. 在讨论正交性时，定义 Young 对称子大小是重要的. 若两 Young 图对应的配分为$[f_1, f_2, \cdots]$与$[f'_1, f'_2, \cdots]$，逐步考察$(f_i - f'_i)$，其中第一个不为零的差是正的，则$[f]$对应 Young 图大于$[f']$Young 图. 反之，Young 图$[f]$小于 Young 图$[f']$. 对于同属一个 Young 图的诸 Young 盘，将第二行数字

放在第一行的右边，第三行数字又放在第二行的右边，则应有 N 个数字. 对应 N 个数字较大者，称为较大的 Young 盘. 若 Young 图 C 大于 Young 图 C'，或 Young 盘 C 大于 Young 盘 C'，则有

$$C' \cdot C = 0.$$

例 4.5.3 Young 图$[3,2,0^3]$对应 5 个 Young 盘，按标号小者较小的规则编号，应为

$$C^{(1)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 4 & 5 & \\ \cline{1-2}\end{array}\,; \quad C^{(2)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 4 \\ \hline 3 & 5 & \\ \cline{1-2}\end{array}\,; \quad C^{(3)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 5 \\ \hline 3 & 5 & \\ \cline{1-2}\end{array}\,;$$

$$C^{(4)} = \begin{array}{|c|c|c|}\hline 1 & 3 & 4 \\ \hline 2 & 4 & \\ \cline{1-2}\end{array}\,; \quad C^{(5)} = \begin{array}{|c|c|c|}\hline 1 & 3 & 5 \\ \hline 2 & 4 & \\ \cline{1-2}\end{array}\,.$$

显然，

$$C^{(5)} \cdot C^{(4)} = C^{(4)} \cdot C^{(3)} = C^{(3)} \cdot C^{(2)} = C^{(2)} \cdot C^{(1)} = 0.$$

但是，

$C^{(4)} \cdot C^{(5)} \neq 0$（正交性不要求 $C^{(4)} \cdot C^{(5)} = 0$，等）.

由于 $y_1 = E - R_{15} y_5, y_i = E(i = 2,3,4,5)$，但 R_{15} 是将 $C^{(5)}$ 变为 $C^{(1)}$ 的置换

$$R_{15} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{bmatrix} = (2453) = [(24)(35)](34),$$

即 $y_1 = E - (24)(35)$，注意(34)为 $C^{(5)}$ 中纵向置换而在 $C^{(1)}$ 的横向置换中没有者. 故得相应的正交等幂元为

$$\left(\left(\frac{d(\lambda)}{n!}\right) = \frac{5}{5!} = \frac{1}{24}\right).$$

$$P_{[f]}^{(1)} = \frac{1}{24} C^{(1)}[f][E - (2,4)(3,5)],$$

$$P_{[f]} = \frac{1}{24} C^{(i)}[f] \quad (i = 2,3,4,5).$$

正交等幂元构成群空间的完备集合

$$E = \sum_{[f]} \sum_i P_{[f]}^{(i)} = \frac{1}{n!} \sum_{[f]} d(\lambda) \sum_i C^{(i)}[f] y^{(i)}[f].$$

S_n 群有 2 个一维表示，一个是用一列 Young 图表示$[n]$的全对称表示（恒等表示），另一个是用分 Young 图表示的$[1^n]$的全反对称表示，设 $f(1,2,\cdots,n)$ 为 n 个对象（粒子）的函数，则全对称函数

$$\Psi^n \equiv Sf \equiv \sum_{g_a \in S_n} P_a f(1,2,\cdots,n),$$

全反对称函数

$$\Psi^{[1^n]} \equiv \hat{A}f \equiv \sum_{g_a \in S_n} (-1)^p P_a f(1,2,\cdots,n);$$

其中，p 为置换 P_a 相应的对换的次数，在 Young 盘计算，尤其是 $SU(n)$ 等计算中，常常略而不计. 更一般地，有福克条件. 表明由于对称或反对称化造成的同一 Young 图的各 Young 盘之间的关联. 设 Young 对称子 $c[f]$ 中，其第 j 行与 i 行各 f_j 格和 f_i 格，且 $f_j \geqslant f_i$，现在第 j 行 u 列和第 i 行 v 列填上数字 a_u 与 b_v，则有

$$[E + \sum_{u=1}^{f_j} (a_u b_v)]c[f] = 0,$$

此式实际上表明，在 $c[f]$ 中，将 b_v 与所有 a_u 全对称化会得到零的结果. 设 Young 盘 $c[f]$ 中第 i 行和 i' 列各有 r_i 与 $r_{i'}$ 格，$r_i \geqslant r_{i'}$，在 μ 行 i 列与 v 行 i' 列填入数字 c_u 与 c_v，则有

$$c[f][E - \sum_{u=1}^{r_i} (c_u d_v)] = 0.$$

此式反映，在 $c[f]$ 中将 c_u 与所有 d_v 反对称化会得到零.

例 4.5.4 $c\left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\right) = -c\left(\begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array}\right)(1,2) = -(1,2)c\left(\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}\right)$,

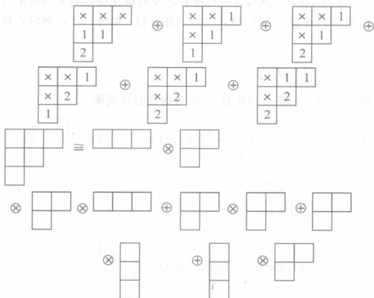
$$\begin{aligned} c\left(\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 \\ \cline{1-1}\end{array}\right) &= c\left(\begin{array}{|c|c|}\hline 2 & 1 \\ \hline 3 \\ \cline{1-1}\end{array}\right)[(1,2)+(1,3)] \\ &= (1,2)c\left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\right) - (1,3)c\left(\begin{array}{|c|c|}\hline 2 & 3 \\ \hline 1 \\ \cline{1-1}\end{array}\right) \\ &= c\left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\right) - (3\ 2\ 1)c\left(\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}\right) \\ &= c\left(\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 \\ \cline{1-1}\end{array}\right) - (2,3)c\left(\begin{array}{|c|c|}\hline 1 & 3 \\ \hline 2 \\ \cline{1-1}\end{array}\right). \end{aligned}$$

$$c\left(\begin{array}{|c|c|}\hline 3&1\\\hline 2&\\\cline{1-1}\end{array}\right)=(2,3)c\left(\begin{array}{|c|c|}\hline 2&1\\\hline 3&\\\cline{1-1}\end{array}\right)(2,3)$$

$$=-(2,3)c\left(\begin{array}{|c|c|}\hline 1&2\\\hline 3&\\\cline{1-1}\end{array}\right)+c\left(\begin{array}{|c|c|}\hline 1&3\\\hline 2&\\\cline{1-1}\end{array}\right)\text{（代入上式）}.$$

作为对称群的约化、Young 氏基、标准基的综合训练，再举一例.

例 4.5.5　S_6 群的表示[3,2,1]按 $S_3\otimes S_3$ 群的不可约表示约化. 按里氏规则，从相反的程序出发，



相应表示维数，

$$16=1\times 2+2\times 1+2(2\times 2)+2\times 1+1\times 2.$$

问题 4.5

1. 在例 4.5.1 中的对称化条件 $\psi_{\mu\nu\lambda}=\psi_{\nu\mu\lambda}$ 与全反对称条件

$$\psi_{\mu\nu\lambda}+\psi_{\nu\lambda\mu}+\psi_{\lambda\mu\nu}=0$$

可以用 Young 对称子表示吗？它与福克条件有何关系？

2. 如果重新定义 Young 对称子为 $c'[f]=a[f]\cdot b[f]$，并令

$$\varphi_{\mu\nu\lambda} = \frac{1}{\sqrt{3}}(\psi_{\mu\lambda\nu} - \psi_{\nu\lambda\mu}),$$

则有反对称条件

$$\text{(i)}\varphi_{\mu\nu\lambda} = -\varphi_{\nu\mu\lambda};\quad \text{(ii)}\varphi_{\mu\nu\lambda} + \varphi_{\nu\lambda\mu} + \varphi_{\lambda\mu\nu} = 0.$$

后一条件保证全反对称组合 $\begin{array}{|c|}\hline \mu \\ \hline \nu \\ \hline \lambda \\ \hline \end{array}$ 被剔去. 试用 $c'[f]$ 解例 4.5.1.

3. 求 S_4 的 Young 不可约表示$[2,1^2]$的 Young 氏基和不可约表示距阵.

提示:有 3 个 Young 盘,相应 Young 对称子,

$$c^{(1)}[2,1^2] = [E - (1,3) - (1,4) - (3,4) + (1\ 3\ 4) + (1\ 4\ 3)][E + (1,2)];$$
$$c^{(2)}[2,1^2] = [E - (1,2) - (1,4) - (2,4) + (1\ 2\ 4) + (1\ 4\ 2)][E + (1,3)];$$
$$c^{(3)}[2,1^2] = [E - (1,2) - (1,3) - (2,3) + (1\ 2\ 3) + (1\ 3\ 2)][E + (1,4)].$$

3 个 Young 氏基为 $\psi_1 = c^{(1)}[2,1^2]\varphi(1,2,3,4)$;$\psi_2 = c^{(2)}[2,1^2]\varphi(1,2,3,4)$;$\psi_3 = c^{(3)}[2,1^2]\varphi(1,2,3,4)$. 由于$(1,2)\psi_1 = \psi - \psi_2$,$(1,2)\psi = -\psi_2 + \psi_3$,$(1,2)\psi_3 = -\psi_3$,故

$$\Gamma^{[2,1^2]}(2,1) = \begin{pmatrix} 1 & 0 & 0 \\ -1 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix};$$

$$\Gamma^{[2,1^2]}(1,3) = \begin{pmatrix} -1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix};$$

$$\Gamma^{[2,1^2]}(1,4) = \begin{pmatrix} -1 & 0 & 1 \\ 0 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix};$$

$(132) = (12)(13)$,$(1432) = (12)(13)(14)$,$(14)(23) = (14)(132)(2)$,等等.

4. 利用 Young 图作外积分解:

(1) $\boxed{3^2} \otimes \boxed{3}$;

(2) $[2,1] \otimes \boxed{1^3}$.

5. 证明:

(1) $[2,1] = [2] \otimes [1] \ominus [3]$;

(2) $[f] \otimes [2,1] = [f] \otimes \{[2] \otimes [1] \ominus [3]\}$;

(3) $[f] \otimes [3,1] = [f] \otimes \{[3] \otimes [1] \ominus [4]\}$,

此处 $\ominus$ 表示剔去某 Young 图.

6. 完成外积分解：



并写出相应的维数等式，并将最后结果所代表的不可约表示用标准基和 Young 氏基表示之.

第5章 分子对称群

我们首先介绍分子对称群，再系统地研究空间对称操作和晶体的对称性，讨论点群的一般特征与分类．首先直观地描述空间对称性．如果在有限几何形体的所有对称操作中，至少有一点不动，则相应的对称操作构成的群称为点群．

在研究空间对称操作时，以不动点为坐标原点，建立坐标系．所有保持空间任一点矢径的长度不变的对称变换集合构成三维实正交群 $O(3)$，点群实质上是其子群．

§5.1 简单的分子对称群

分子对称群就是由分子的对称操作构成的群．如果分子 M 的对称操作构成点群 G，就说分子 M 属于点群 G．在这一节里，我们要弄清楚实际上存在哪些分子对称群和如何确定一个分子所属的对称群．

定义 5.1.1 对称操作据以进行的几何元素称为物体的对称元素．

例如，旋转是绕某一轴（直线）进行的，反射是对某个平面进行的，平移是沿某一矢量进行的，等等．

定义 5.1.2 如果绕通过物体的一条直线旋转（$2\pi/n$），使物体复原，则说直线是物体的一个 n 重（旋转）轴，记作 C_n．n 最大的 C_n 轴称为主轴．

定义 5.1.3 如果有一个通过物体平面，物体对这一平面的镜像与其自身重合，则说这个平面是物体的一个对称面（或镜面），记作 σ，对这一平面的反射操作也记作 σ．

定义 5.1.4 如果旋转轴和镜面 σ_h 互相垂直，旋转（$2\pi/n$）之后接着进行一次反射 σ_h 能使物体复原，这种复合对称操作就叫做像转，记作 S_n．特别地，二重像转 $S_2 = C_2\sigma_h = \sigma_h C_2$ 就是反演，记作 I．

定义 5.1.5 如果分子对称群中存在操作使它的对称元素 ε_X 和 ε_Y 换位置，即 ε_X 和 ε_Y 是共轭对称元素，互相共轭的对称元素的集合组成共轭对称元素系．

1. 单轴群

只有一个 n 重旋转轴或像转轴．无轴群（$n = 1$，只能进行旋转）和回转群（$n \to \infty$，

可作无穷小角度旋转，即可作任意角度旋转）可看作它的两种极端情况.

(1)C_n

若分子只有一个 n 重旋转轴，它就属于 C_n 群，群元素为 $\{E, C_n, C_n^2, \cdots, C_n^{n-1}\}$. 这是 n 阶循环群，每个元素自成一类，共有 n 类. 属于这一点群的分子如 H_2O_2[图 5.1(a)]，$Cl_2C—CH_2$[图 5.1(b)]，H_2S_2，$CH_3O—OCH_3(C_2)$ 以及 $N(SiH_3)_3(C_3)$ 等.

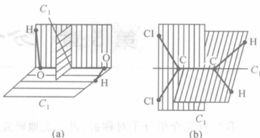


图 5.1　某些单轴群的对称元素图

当 $n = 1$ 时，实际上没有对称轴，但形式上也记成 C_1 群，例如 CHFClBr，$Br_2CH—CH_2Br$ 等.

在 C_n 的基础上若再有对称面，在保证不增加新的旋转轴（因为已假定只有一个旋转轴）的条件下，只有三种可能：一是产生像转轴 $S_{2n}, S_{2n}^2 = C_n$，二是垂直 C_n 轴，三是通过 C_n 轴.

(2)S_n

分子只有一个像转轴 S_n，就属于 S_n 群，它也是循环群，若 n 为偶数，$n = 2m$，则有 n 个元素，分为 n 类$\{E, S_{2m}, S_{2m}^2 = C_m, S_{2m}^3, \cdots, S_{2m}^{2m-1}\}$. 属于 S_n 群的分子较少，如 1,3,5,7-四甲基环辛四烯，$C(SCH_3)(S_4)$，折皱的苯，$[Ni(NO_2)_6]^{4-}$（在 $K_4[Ni(NO_2)_6]$ 晶体中）(S_6) 等.

当 $n = 2$ 时，$S_2 = I$，这个群记作 $C_I\{E, I\}$. 例如，BrClHC—CHClBr[图 5.1(d)]，HOOC—COOH(I_8)，二聚甲酸，草酸二甲酯，反式丁二酸，$[Pd(NO_2)_4]^{2-}$（例如在 $K_2[Pd(NO_2)_4]$ 晶体中）等属于 C_I 点群. 当 n 为奇数时，S_n 群就是 C_{nh} 群.

(3)C_{nh}

若分子有一个 n 重旋转轴和一个垂直于旋转轴的镜面（水平镜面），就得到 C_{nh} 群. 这是一个互换群，子群 C_n 和 C_{1h} 的元素彼此可对易，所以 C_{nh} 可看成是 C_n 和 C_{1h} 的直积，$C_{nh} = C_n \otimes C_{1h}$，有 $2n$ 个对称操作，分为 $2n$ 类

$$\{E, C_n, C_n^2, \cdots, C_n^{n-1}, \sigma_h, \sigma_h C_n, \sigma_h C_n^2, \cdots, \sigma_h C_n^{n-1}\}.$$

属于这种点群的分子如 1,4-二氯-2,5-二溴代苯，反式丁二溴乙烯，反式丁二烯 (C_{2h})，$C(NH_2)_3^+$.

当 $n = 1$ 时，就是只有一个对称面，记作 $C_{1h} = C_s\{E, \sigma_h\}$，例如 NBrO，$HNO_2$，HOCl，$HN_3$，$CHClF_2$ 等.

(4)C_{nv}

若分子有一个 n 重旋转轴和通过 C_n 轴的镜面，就得到 C_{nv} 群. 由于 n 重旋转轴的存在，有一个对称面必然要带来其他 $(n-1)$ 个对称面，两个平面的交角为 $1/2\cdot 2\pi/n$. 当 n 为奇数时，这是显然的. 当 n 为偶数时，乍看似乎只有 $n/2$ 个对称面 σ_v，相邻两个镜面的交角为 $(2\pi/n)$. 当 n 为偶数时，出现反射操作：$C_n^{n/2}\sigma_h = I$，有对称中心. 但实际上当存在 C_n 和 σ_v 时，还必定存在另外一组 $(n/2$ 个$)$ 镜面 σ'_v，$\sigma_v C_n = \sigma'_v$. 这从图 5.2 可以看出，进行操作 C_n 使 $A\to B$，再经过 $\sigma_v^{(2)}$ 反映 $B\to A'$，而 A 和 A' 对于 σ'_v 互为镜像，即 $\sigma_v^{(2)}C_n = \sigma'_v$.

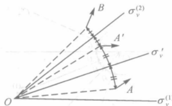


图 5.2 $\sigma_v^{(2)}C_n = (\sigma_v^{(1)})'$，($C_n$ 轴垂直于纸面)

反过来看，上面已经证明过，存在交角为 $1/2\cdot 2\pi/n$ 的两个对称面必然带来 $2\pi/n$ 的旋转，也就是两个平面的交线为 C_n 轴. 所以 C_{nv} 群的对称操作为 $\{E, C_n, C_n^2, \cdots, C_n^{n-1}, \sigma_v^{(1)}, \sigma_v^{(2)}, \cdots, \sigma_v^{(n-1)}\}$ 共有 $2n$ 个操作.

C_n 是双向轴，C_n 和 C_n^{n-1} 属于同一类. 因此，当 n 为奇数时，$2n$ 个元素分为 $(n+3)/2$ 类（所有 σ_v 属于同一类）；当 n 为偶数时，分为 $(n+6)/2$ 类（σ_v 和 σ_v' 分属于两个类）；属于这类点群的分子如 CH_2Cl_2[图 5.3(a)]，H_2O，Cl_2O，O_2，HCHO，船式构象环己烷 (C_{2v})，CH_3Cl[图 5.3(b)]，BrF_3，F_3，PF_3S，NH_3，$CHCl_3$ 及三氯乙烷 (C_{3v}) 等.

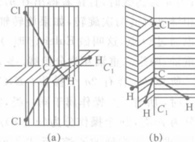


图 5.3 某些双面群分子的对称元素图

(5)C_∞，$C_{\infty v}$

这是 C_n 和 C_{nv} 当 $n\to\infty$ 时的情况. 异核双原子分子或其他没有对称中心的线型分子属于 $C_{\infty v}$ 点群，例如 CO，HCl，HCN 等.

以上就把只有一个旋转轴的情况讨论清楚了.

2. 双面(二面体)群 D_n

如果分子除一个主旋转轴 $C_n(n\geqslant 2)$ 之外还有另外 n 个垂直于 C_n 轴的二重旋转轴，就属于双面群 D_n. 二重旋转轴必须垂直于主旋转轴，否则就不只有一个高于二重的旋转轴. 当主旋转轴 C_n 的 $n>3$ 时，这是显然的，因为二重轴把主旋转轴移到另外的位置，该处原来也必须有一个高重旋转轴. 即使主旋转轴是二重的，也是如此. 设另一个二重轴和主旋转轴交角为 $\theta(\theta\neq\pi/2)$，则必定再有一个与主旋转轴相交为 2θ 的旋转轴. 由这个二重轴又带出另一个，…，如图 5.4 所示.

最后若共有 n 个二重轴，必须满足 $2n\theta = 2\pi$ 的要求，所以垂直于这些二重轴必然有

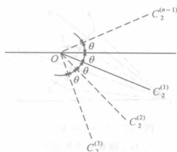


图 5.4　不互相垂直的二重轴产生高重旋转轴

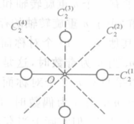


图 5.5　由 C_4 和 C_2 轴产生 C'_2 轴（C_4 轴垂直纸面）

一个 n 重轴. 这说明原来选二重轴为主轴不对. 垂直于 C_n 轴若有一个二重轴，必然带来另外$(n-1)$个二重轴，相邻两个二重轴的夹角为 $1/2 \cdot 2\pi/n$. 当 n 为奇数时，这是显然的；当 n 为偶数时，直接看得出有 $n/2$ 个二重轴，而根据旋转乘积的 Euler 定理（绕不同轴相继进行的两次旋转，如果旋转轴相交于一点 O，则其结果等效于一个旋转，它的旋转也通过 O 点，这叫做 Euler 定理.），C_n 轴和这 $n/2$ 个二重轴相乘产生另外一组 $n/2$ 个二重轴，两组二重轴互为分角线. 举 D_4 的情况为例（图 5.5）.

所以 D_n 群有 $2n$ 个操作 $\{E, C_n, C_n^2, \cdots, C_n^{n-1}, C_2^{(1)}, \cdots, C_2^{(n)}\}$. C_n 为双向轴，当 n 为奇数时，所有 $C_2^{(i)}$ 操作属于同一类，$2n$ 个操作分为 $(n+3)/2$ 类；当 n 为偶数时，$C_2^{(i)}$ 操作分为两类，$2n$ 个操作分为 $(n+6)/2$ 类. D_n 和 C_{nv} 同构. 属于这一点群的分子如扭曲的乙烯、非平衡构型的乙烷、反式 $[Co(NH_3)_2(NH_3)_2(NO_2)_4]^-$（在 $K[Co(NH_3)_2(NO_2)_4]$ 晶体中，不算 H，D_4）等.

3. 立方体群

当有多个$(n \geqslant 3)C_n$ 轴时，可能实现哪些对称元素的组合呢？假定有 n 个高重旋转轴，选取其中两个交角最小者，例如，分别是 C_n 和 C_m 轴. 以这两个轴的交点为球心作球面，分别与这两个旋转轴相交于 A，B 两点. 若绕 OA 轴作 $C_n^i (i=1,2,\cdots,n-1)$ 旋转，则 OB 轴被移置 n 个方向，设它们与球面的交点为 $B, B^{(1)}, B^{(2)}, \cdots, B^{(n-1)}$. 同样，如果绕 OB 轴作 $C_m^j (j=1,2,\cdots,m-1)$ 旋转，则 OA 轴被移置 m 个方向，设它们与球面的交点为 $A, A^{(1)}, \cdots, A^{(m-1)}$. 若再用某一个 $OA^{(j)}$ 为轴作 C_n 旋转，则这个 $OA^{(j)}$ 轴周围必然又均匀围着 n 个 OB 轴. 同样，每个 OB 轴周围也必然均匀围绕着 m 个 OA 轴.

如果用通过球心的平面在球面上切出的圆弧把相邻的 B 点连接起来，就可以得到球面正凸 n 边形，其中心是 OA 轴. 球面必然被若干个这种正凸 n 边形所布满，否则将有

一些 OB 轴不能通过绕 OA 轴作 C_n 旋转换位置，破坏假设的前提. 于是，若把所有互相邻近的 B 点都用直线连接起来，我们将得到一个内接于球面的由正凸 n 边形围成的正凸多面体，它的顶角将是由 m 个面围成的，因为通过每个正 n 边形的中心有一个 OA 轴，而围绕着一个 OB 轴的最邻近的 OA 轴有 m 支. 显然正凸多面体的各个面、各条棱、各个顶点分别相互等价. 图 5.6 表示 $n=5, m=3$ 的情况.

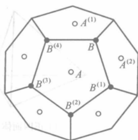


图 5.6　有多个三重轴和五重轴的情况

n 和 m 要满足一定条件才能构成正凸多面体. 围成正凸多面体一个顶点的 m 个正 n 边形的顶角之和为：

$$s = m(n-2)\pi/n.$$

要围成凸顶角，必须 $s < 2\pi$，能满足这种条件的 m 和 n 的组合只有五种(表 5.1)。

表 5.1

n	m	正多面体的形状
3	3	正四面体
3	4	正八面体
3	5	正(三角)二十面体
4	3	立方体
5	3	正(五角)十二面体

这样我们就证明了具有两个以上高重旋转轴的分子，其共轭旋转轴系必与某一个正凸多面体的相同，而能够存在的满足对称性条件的正凸多面体只有这五种(图 5.7). 下面分别讨论.

(1) 正四面体群

1)T：检查正四面体[图 5.8(b)]可以找出它的共轭旋转轴系，计有：四个通过它的一个顶点和相对着的平面中心的三重轴，三个互相正交的(通过不相邻的两条棱中点的)二重轴. 所以它有十二个旋转操作：

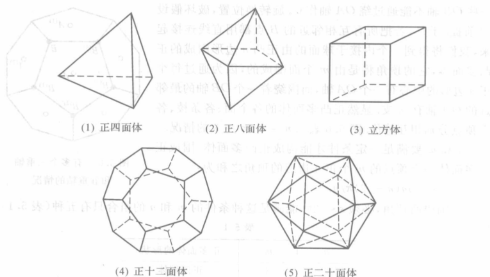
$$\{E, 4C_3, 4C_3^2, 3C_2\},$$

这些对称操作构成了 T 群. 三重轴是单向轴，但各三重轴和二重轴可以通过对称操作 各自换位置，所以它们的相同对称操作属于同一类，共分四类. 新戊烷 $C(CH_3)_4$ 分子中，甲基不处于最高的对称位置(旋转角 φ) 时，即属于 T 群[图 5.8(a)].

在 T 群中引入对称面时，为了保证不产生新的旋转轴，它只能垂直于一个二重轴(同时也就通过另外两个二重轴)，或者通过一个二重轴同时平分另外两个二重轴的夹角.

2)T_h：当对称面垂直于一个二重轴时，对称面一定有三个：

$$C_2\sigma_h = S_2 = I,$$



(1) 正四面体　(2) 正八面体　(3) 立方体

(4) 正十二面体　(5) 正二十面体

图 5.7　五种正多面体

有对称中心. 反射操作与任何操作可对易(即可交换),所以 T_h 可视为 T 和 C_I 的直积:

$$T_h = T \otimes C_I.$$

由此得知它的对称操作共有 24 个,分 8 类:

$$\{E, 4C_3, 4C_3^2, 3C_2, I, 4IC_3 = 4S_6^5, 4IC_3^2 = 4S_6; 3IC_2 = 3\sigma_h\}.$$

可举$[Co(NO_2)_6]^{3-}$ 离子(在 $K_3[Co(NO_2)_6]$ 晶体中)作为 T_h 群的例子.

3)T_d:当对称面 σ_d 通过一个二重轴并平分另外两个二重轴的夹角时,得到 T_d 群[图 5.8(b)],σ_d 有六个. 由于平分两个二重轴的夹角并通过另一个二重轴的对称面的存在,这后一个二重轴转化为四重像转轴,显然有三个,是双向轴. σ_d 通过 C_3,也使 C_3 变成双向轴,所以 T_d 群的 24 个对称操作分为五类:

$$\{E, 3C_2, 8C_3, 6S_4, 6\sigma_d\}.$$

T_d 群完全反映了一个正四面体的对称性,它与置换群 S_4 同构. 属于 T_d 点群的分子很多,如 CH_4,CCl_4,NH_4^+,MnO_4^-,$TiCl_4$,$SnBr_4$,SiF_4,P_4O_5,P_4O_{10} 等.

当甲基(—CH_3)处于最高对称位置时,$Si(CH_3)_4$,$C(CH_3)_4$ 等分子也属于 T_d 点群.

(2) 正八面体群

1)O:从图 5.8(d) 可见,正八面体的共轭旋转轴系计有三个四重轴(分别通过相对的两个顶点)、六个二重轴(分别通过相对的两边的中点)、四个三重轴(分别通过相对的两个面的中心). 由这些对称元素的对称操作构成的群称为 O 群,共有 24 个对称操作.

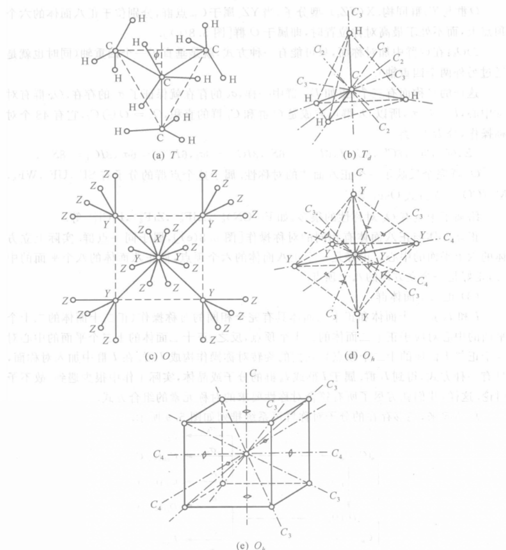


图 5.8　立方体群的对称元素图

它的旋转轴都是双向轴，所以对称操作分为五类：

$$\{E, 6C_4, 3C_4^2 = 3C_2, 6\,C_2', 8C_3\}.$$

O 群与 T_d 群同构. $X(YZ_4)_6$ 型分子，当 YZ_4 属于 C_{4v} 点群，分别位于正八面体的六个顶点上，而不处于最高对称位置时，即属于 O 群[图 5.8(c)].

2)O_h：在 O 群中加对称面，只可能有一种方式，就是垂直于一个四重轴(同时也就是通过另外两个四重轴).

这样的对称面有三个，正如 D_{nh} 群中一样，σ_h 的存在就保证了 σ_v 的存在. O_h 群有对称中心，$I = C_2\sigma_h$，所以 O_h 群可看成是 O 群和 C_I 群的直积，$O_h = O \otimes C_I$，它有 48 个对称操作，分为 10 类：

$\{E, 6C_4, 3C_2, 6C'_2, 8C_3; I, 6IC_4 = 6S_4, 3IC_2 = 3\sigma_h, 6IC'_2 = 6\sigma_v, 8IC_3 = 8S_6\}$.

O_h 群完全反映了一个正八面体的对称性. 属于这个点群的分子有 SF_6，UF_6，WF_6，$Mo(CO)_6$，立方式 OsF_8 等，

络离子中具有 O_h 对称性的很多，如 $Fe(CN)_6^{4-}$，AlF_6^{2-}，ZrF_6^{2-}，$PtCl_4^{2-}$ 等.

正立方体与正八面体有相同的对称操作[图 5.8(e)]，属于同一点群. 实际上立方体的六个平面的中心，正好是一个正八面体的六个顶点，而正八面体的八个平面的中心，正好是一个立方体的八个顶点.

(3) 正二十面体群

I 和 I_h 正二十面体和正十二面体具有完全相同的对称操作(正二十面体的二十个平面的中心对应于正十二面体的二十个顶点，反之，正十二面体的十二个平面的中心对应于正二十面体的十二个顶点)，它们的旋转对称操作构成 I 群. 在 I 群中加入对称面，只有一种方式，得到 I_h 群. 属于 I 群或 I_h 群的分子或晶体，实际工作中很少遇到，故不予讨论. 这样，我们就穷尽了所有符合对称性要求的对称元素的组合方式.

总结起来，能够存在的分子对称群可系统排列如图 5.9 所示.

$C_n(C_I, C_\infty)$ —σ_h→ S_{2n}；—σ_h→ $C_{nh}(C_v, C_I)$；—σ_v→ $C_{nv}(C_{\infty v})$

$C_n(C_I, C_\infty)$ —C_2'→ $D_n(D_\infty)$ —σ_h→ $D_{nh}(D_{\infty h})$；—σ_d→ D_{nd}

C_n —C_m→ T —σ_h→ T_h；—σ_d→ T_d

C_n —C_m→ O —σ_h→ O_h

图 5.9　分子对称群

实际存在的分子对称群中，旋转轴 C_n 的重数 n 只取几个数值. 除 $n\to\infty$ 的特例之外，单轴群和双面群中，n 只取值 1,2,3,4,5,6;7 和 8 就很少碰到了. 当有多个高重旋转轴时，n 只取值 2,3 或 4.

§ 5.2　空间的对称性

我们首先直观地描述空间对称性. 如果在有限几何形体的所有对称操作中，至少有一点不动，则相应的对称操作构成的群称为点群. 对称操作的概念及相应乘法的定义在前面已经叙述过了.

以不动点为坐标原点，建立坐标系. 所有保持空间任一点矢径长度不变的对称变换集合构成三维实正交群 $O(3)$，点群实质上是其子群.

设矢径 $x = x_1e_1 + x_2e_2 + x_3e_3$，其中 $e_i, e_j = \delta_{ij}(i, j = 1,2,3)$，或用列矩阵表示. 试用 3×3 矩阵 $\{a_{ij}\}$ 表示三维定点转动，即

$$\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{2.1}$$

$$x'_\mu = a_{\mu\nu}x_\nu (\mu, \nu = 1,2,3),$$

矢径长度不变，即

$$x'^2_1 + x'^2_2 + x'^2_3 = x_1^2 + x_2^2 + x_3^2,$$

$$\sum_{\sigma,\nu=1}^{3} \delta_{\sigma\nu}x_\sigma x_\nu = \sum_{\nu,\sigma=1}^{3} a_{\mu\sigma}a_{\mu\nu}x_\sigma x_\nu.$$

对比两边，得到

$$\sum_\mu a_{\mu\sigma}a_{\mu\nu} = \delta_{\sigma\nu} \Rightarrow \tilde{a}_{\sigma\mu}a_{\mu\nu} = (\tilde{A}A)_{\sigma\nu} = \delta_{\sigma\nu},$$

用矩阵表示上式，即为 $\tilde{A}A = E$，由此式可知，变换矩阵集合 $\{A\}$ 正是 $O(3)$ 群. 由 $\tilde{A}A = E$ 得，$\det A = \pm 1$. $\det A = 1$，表示纯转动. 只含纯转动元素的点群称为第一类点群；$\det A = -1$，对应纯转动与空间反射元素的组合称为第二类点群.

如果将固定点条件放弃，(2.1) 式推广到下式

$$\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}, \tag{2.2}$$

它表示空间一般操作. 若 (2.2) 式中，$a_{13} = a_{23} = a_{31} = a_{32} = 0, a_{33} = 1, b_1 = b_2 = 0$，则表示绕第三轴的转动，并沿此轴平移 b_3，这种操作叫螺旋转动. 若所有的 $a_{ij} = 0$，则

表示空间纯平移操作. 此类操作可视为螺旋转动的特例. 螺旋转动含纯转动元素，称为第一类操作，见图 5.10 所示.

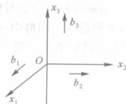


图 5.10

若(2.2)式简化为

$$\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ 0 \end{pmatrix}, \tag{2.3}$$

由于 $\det A = -1$，相应操作称为第二类操作. 上式表示对 x_1-x_2 平面反映并沿 x_1-x_2 平面有滑移(b_1, b_2).

当上式变为

$$\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{2.4}$$

时，则表示沿 x_3 轴转动 α 角，并对平面 x_1-x_2(垂直于 x_3 轴）进行反映. 这种操作称为转动反映，也属第二类操作. 上式中令 $\alpha = \pi + \beta$，则矩阵 A 可表示为沿第三轴转动 β 的矩阵与反射矩阵$(-E)$的乘积，即操作变为沿 x_3 转动 β 角，再相对原点反演，称为转动反演.

综上所述，任一空间操作，可分为三大类：螺旋转动（包含平移）、滑移反映与旋转反演. 除第一种为第一类操作外，其余两种属于第二类操作.

因此空间操作有 8 种：

(1) 反演（相对于对称中心）——i，

(2) 反映（相对于映面 $\boldsymbol{m}$）——$\sigma(\boldsymbol{m})$，

(3) 旋转（相对于转轴 $\boldsymbol{n}$）——$C(\boldsymbol{n}, \alpha)$，

(4) 旋转反演 ——$iC(\boldsymbol{n}, \alpha)$，

(5) 旋转反映 ——$S(\boldsymbol{n}, \alpha) = \sigma(\boldsymbol{n})C(\boldsymbol{n}, \alpha) = iC(\boldsymbol{n}, \alpha + \pi)$，

(6) 平移 ——$(\alpha|t)$，其中 α 表示对原点的操作，相当于(2.2)式中$\{a_{ij}\}$，t 表示纯平移，相当于(b_1, b_2, b_3)，

(7) 滑移反映 ——$i(\alpha|t)$，

(8) 螺旋旋转 ——$(\alpha|t) \cdot C(\boldsymbol{n}, \alpha)$.

其中前 4 种是点操作. 在这 4 种操作中，只有纯旋转为第一类操作，其余为第二类操作.

在纯转动中，对于晶体受到晶格周期性的限制，转角只能是$\frac{2\pi}{n}$，其中整数 $n = 1, 2, 3, \cdots$，当 $n = 2, 3, \cdots$ 时，分别把转轴 $\boldsymbol{n}$ 称为二度、三度等轴，相应转动记为 $C_2, C_3, \cdots, C_n$.

在镜面反映中，反射面与 C_n 轴垂直记为 σ_h；反射面通过转轴 C_n 者记为 σ_v. 如果 σ_h 为独立元素，则 $C_2\sigma_h = i$，其中 i 的反演中心为转轴与映射面 σ_h 相交的点. 同样，$C'_n\sigma_h = S(\boldsymbol{n})$，$(C'_n\sigma_h)^2 = (S(\boldsymbol{n}))^2$，等等.

其中点操作有如下运算性质：

$$\begin{cases} i^2 = I(\text{恒等操作}), \\ \sigma(\boldsymbol{m})^2 = I, \\ \sigma(\boldsymbol{m}_1)\sigma(\boldsymbol{m}_2) = c(\boldsymbol{m}_1 \times \boldsymbol{m}_2, 2\varphi(\boldsymbol{m}_1, \boldsymbol{m}_2)), \end{cases}$$

其中 φ 为法线 $\boldsymbol{m}_1$ 与 $\boldsymbol{m}_2$ 的夹角. 显然

$$\begin{cases} i\sigma(\boldsymbol{m}) = C(\boldsymbol{m}, \pi), \\ C(\boldsymbol{n}, \beta) \cdot C(\boldsymbol{n}, \alpha) = C(\boldsymbol{n}, \alpha + \beta), \\ C(\boldsymbol{n}_1, \alpha) \cdot C(\boldsymbol{n}_2, \beta) = C(\boldsymbol{n}_3, \gamma), \end{cases}$$

其中 $\frac{\alpha}{2}$，$\frac{\beta}{2}$ 和 $\frac{\gamma}{2}$ 为 $\boldsymbol{n}_1$、$\boldsymbol{n}_2$ 与 $-\boldsymbol{n}_3$ 在单位球面上形成球面三角形的三内角；此外还有

$$\begin{cases} ig = gi(g\ \text{为任意操作}), \\ g^{-1}\sigma(\boldsymbol{m})g = \sigma(g\boldsymbol{m}), \\ g^{-1}C(\boldsymbol{n}, \alpha)g = C(\pm\, g\boldsymbol{n}, \alpha). \end{cases}$$

关于点群共轭类的划分，前面已介绍三种判别方法，现进一步讨论如下：

(1) 关于不同转轴 C_n 与 C'_n 的转动元素. 容易证明，如果存在 C_n 轴与垂直于它的二阶轴(C'_2)，则必存在 n 个垂直于它的二阶轴. 有鉴于此，若存在另一个转轴 C'_m(可能与 C_n 有一定交角)，则由乘法的封闭性，有

$$(C'^i_m)^{-1}C^k_nC'^i_m \equiv C'^k_n \in G,$$

即在群 G 中存在等价的转轴 C'_n，而且由于 $C^i_m \in G$，$(i = 1, 2, \cdots, m)$，会产生 m 条 n 阶等价轴. 相对于这些等价转轴的相同转角元素均为同一共轭类. 反之，C_n 轴也会产生与 C'_m 等价的 n 条转轴，相对这些转轴的相同转角元素亦属同一类.

其中一个特例是 C'_m 为与 C_n 轴垂直的 C'_2 轴，则

$$(C^1_2)^{-1}C^k_nC'_2 \equiv C^{-k}_n(C'^k_n),$$

注意到 $C'_2 = (C'_2)^{-1}$，得 $C'^{-k}_n = C'^k_n$，可见 C_n 与 C'_n 轴重合，但反向(转动反向)，这样的轴叫双向轴.

(2) 关于不同反射面的反射元素的共轭元，若反射面 σ_h 垂直于转轴 C_n，则由于

$$C^k_n\sigma_h = \sigma_hC^k_n,$$

此时不会产生新的共轭元. 若反射面 σ_v 通过 C_n 轴，则由于 $\sigma_v = iC_2$，且 i 与所有操作元素对易，应有

$$\sigma_v^{-1}C^k_n\sigma_v = \sigma_vC^k_n\sigma_v = C_2C^k_nC_2 = C^{-k}_n,$$

亦即 C_n 轴成为双向轴. 若既不存在与 i 垂直，又不存在通过它的反射面 σ_v，则转轴一定为单向轴.

注意，当存在通过 C_n 轴的反射面 σ_v 时，则必存在 n 个通过转轴的等价反射面. 事实上，

$$(C_n^i)^{-1}\sigma_v C_n^i = \sigma_v',$$

若 $i = 1,2,\cdots,n$，分别产生 n 个等价反射面.

我们一般称转轴 C_n 为 n 次轴. 一次轴即恒等变换 i 在晶体点群中，由于空间周期性结构，只存在一次、二次、三次、四次及六次轴. 以后我们要证明这一点.

问题 5.2

1. 证明：若相交 O 点的两个二次轴 C_{2A} 与 C_{2B} 夹角为 θ，C 轴垂直于 C_{2A} 与 C_{2B} 所在的平面，则有关系 $C'_{2B}C'_{2A} = C_C(2\theta)$，其中 $C_C(2\theta)$ 表示操作：绕 C 轴转动 2θ.

[提示：设 A 为 Ox 轴，B 轴单位矢为 i_B，则用并矢表示 $C'_{2A} = ii + [jj + kk]\cos\pi =$

$$ii - jj - kk = 2ii - E = \begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{vmatrix}, i_B = i\cos\theta + j\sin\theta.$$

类似于上式有 $C'_{2B} = 2i_B i_B - \vec{E}\ (\vec{E} = \vec{ii} + \vec{jj} + \vec{kk})$，

$$\begin{aligned} C'_{2B}(C'_{2A}r) &= [2i_B i_B - \vec{E}][2(ii - \vec{E})r] \\ &= r + 4i_B(i_B i)(ir) - 2i_B(i_B i) - 2i(ir) \\ &= i(x\cos 2\theta - y\sin 2\theta) + j(x\sin 2\theta + y\cos 2\theta) + kz. \end{aligned}$$

但用并矢表示的绕 Oz 轴转动 φ 的操作是

$$C_C(\varphi) = kk + (ii + jj)\cos\varphi + \vec{E}\times k\sin\varphi,$$

$$C_C \cdot r = i(x\cos\varphi - y\sin\varphi) + j(y\cos\varphi + x\sin\varphi) + kz.]$$

2. 证明：对于平面 A 与 B 的两个反射 σ_A 与 σ_B 的乘积，等价于绕两平面交线的转动，转角等于两平面交角的两倍，即 $\sigma_A\sigma_B = C(2\varphi_{AB})$.

[提示：设两平面法线矢量 $n_A = i, n_B = i\cos\theta + j\sin\theta, \theta = \varphi_{AB}$，则

$$\sigma_A = \vec{E} - 2n_A \cdot n_A, \sigma_B = \vec{E} - 2n_B \cdot n_B,$$

$$\sigma_A(\sigma_B r) = i(x\cos 2\theta - y\sin 2\theta) + j(y\cos 2\theta + z\sin\varphi) + kz,$$

此外，交线单位矢为 k，$C(k) = kk + (\vec{E} - kk)\cos\varphi + (\vec{E}\times k)\sin\varphi$，

$$C(k)r = i(x\cos\varphi - y\sin\varphi) + j(y\cos\varphi + z\sin\varphi) + kz.]$$

3. 证明：一个转动 φ 的操作与通过转轴平面 A 的反射 σ_A 的乘积，等于过该轴的另一平面 B 的反射 σ_B，A 与 B 的夹角为 $\varphi/2$.

[提示:令转轴 $n=i$,则 $C(\varphi)=ii+(jj+kk)\cos\varphi-[-jk+kj]\sin\varphi$. 令平面 A 法向 $\boldsymbol{n}_A=j$,则 $\sigma_A=\vec{E}-2jj=ii+kk-jj$.

$$C(\varphi)r=ix+(jy+kz)\cos\varphi+[-jz+ky]\sin\varphi,$$

$$\sigma_A=[C(\varphi)r]=ix-k(z\cos\varphi+y\sin\varphi)-j(y\cos\varphi-z\sin\varphi).$$

设 $\boldsymbol{n}_B$ 与 y 轴夹角为 θ,则 $n_B=j\cos\theta+k\sin\theta$,

$$\begin{aligned}\sigma_B&=\vec{E}-2n_Bn_B=ii+2(j\cos\theta+k\sin\theta)(j\cos\theta+k\sin\theta)\\&=(ii+jj+kk)-2(j\cos\theta+k\sin\theta)(j\cos\theta+k\sin\theta)\\&=ii-jj\cos2\theta-(jk+kj)\sin2\theta+kk\cos2\theta,\end{aligned}$$

$$\sigma_Br=ix-j(y\cos2\theta+z\sin2\theta)+k(z\cos2\theta-y\sin2\theta).$$

当 $\theta=-\varphi/L$ 时,$\sigma_B=\sigma_AC(\varphi)$.]

4. 若在循环转动群中只有五种固有循环群,即在$\{C_n\}$中,$n=1,2,3,4,6$,证明在包含两个或两个以上转轴的固有点群中各次转轴数目 n_i 之间有关系 $n_2=3+n_4+3n_6$.

[提示:C_n 群有 n 个不等价不可约表示,显然有群的阶 $g=1+n_2+2n_3+3n_4+5n_6$,其中各子群有共同元素:恒元. 平庸表示 $Tr\,\Gamma(E)=3$,子群$\{C_n\}$的三维自然表示$\{\Gamma_a^{reg}(n)\}$,在正交归一基中,每个表示矩阵只有一个对角元为 1,其余对角元为零,可以用并矢表为 $\boldsymbol{nnn}$. 由此

$$\sum_{g_a\in G}Tr[\Gamma^{reg}(g_a)]=3+(2-3)n_2+(3-3)n_3+(4-3)n_4+(6-3)n_6,$$

但$[\sum_{g_a\in G}g_a]r=r$,故$[\sum_{g_a\in G}g_a]r$ 是其转轴可以不重合的,$\sum_a g_a=0$.]

5. 试用球坐标导出绕空间任意轴转动 φ 的表达式,见图 5.11.

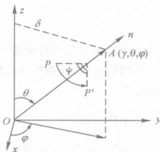


图 5.11

[提示:设转轴 $\boldsymbol{n}$ 的方向余弦为 l、m、n,其中 $l=\sin\theta\cos\varphi$,$m=\sin\theta\sin\varphi$,$n=\cos\theta$. $P(x,y,z)$ 为空间任一点,绕 $\boldsymbol{n}$ 轴转动 ψ 到 $P'=(x',y',z')$. 用符号表示:$r\xrightarrow{R}r'$,或

$$\begin{bmatrix}x'\\y'\\z'\end{bmatrix}=\Gamma(\psi,n)\begin{bmatrix}x\\y\\z\end{bmatrix}.$$

但绕 $\boldsymbol{n}$ 轴的转动 ψ 相当于先将 $\boldsymbol{n}$ 轴移到 Oz 轴(记为 $\Gamma_a(-\theta)$),然后沿 Oz 轴转动 ψ,最后将转轴转回 $\boldsymbol{n}$ 轴,即

$$\Gamma(\psi,n)=\Gamma_a^{-1}\Gamma(\psi,k)\Gamma_a.$$

此外，$\Gamma_a(\theta)$ 又可分为两次操作：先绕 $Oz(k)$ 轴绕 $-\varphi$，再绕 $Oy(j)$ 轴绕 $-\theta$，即得 $\boldsymbol{n}$ 轴转到 Oz 轴.

$$\Gamma_a = \Gamma(-\theta, j)\Gamma(-\varphi, k)$$

$$= \begin{vmatrix} \cos\theta & 0 & -\sin\theta \\ 0 & 1 & 0 \\ \sin\theta & 0 & \cos\theta \end{vmatrix} \begin{bmatrix} \cos\varphi & \sin\varphi & 0 \\ -\sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

易得

$$\Gamma_a^{-1} = \begin{vmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{vmatrix} \begin{bmatrix} \cos\theta & 0 & \sin\theta \\ 0 & 1 & 0 \\ -\sin\theta & 0 & \cos\theta \end{bmatrix},$$

$$\Gamma(\psi, k) = \begin{bmatrix} \cos\psi & -\sin\psi & 0 \\ \sin\psi & \cos\psi & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

结果

$$\Gamma(\psi, n) = \Gamma_a^{-1}\Gamma(\psi, k)\Gamma_a$$

$$= \begin{bmatrix} \cos\psi + l^2(1-\cos\psi) & lm(1-\cos\psi) - n\sin\psi & ln(1-\cos\psi) + m\sin\psi \\ lm(1-\cos\psi + n\sin\psi) & \cos\psi + m^2(1-\cos\psi) & mn(1-\cos\psi) - l\sin\psi \\ ln(1-\cos\psi) - m\sin\psi & mn(1-\cos\psi) + l\sin\psi & \cos\psi + n^2(1-\cos\psi) \end{bmatrix}$$

上式与用并矢表达式 $\Gamma(\psi, n) = nn - (1 - nn)\cos\psi + (\vec{E} \times n)\sin\varphi$ 等效.

§ 5.3　晶格的对称性

晶体结构的基本特征是，构成它们的原子或离子、原子团在空间呈现周期性排列，构成所谓的晶格. 周期性条件促使晶格的对称操作均离散化，不存在连续群中的无穷小操作元素.

1. 平移对称

$\boldsymbol{l}$ 为晶格矢量. 晶体的最小周期单元叫晶胞. 晶胞的 3 个不共面的棱称为晶格基矢，设为 a_1、a_2 与 a_3. 晶格矢量 $\boldsymbol{l}$ 必须表为晶格基矢的线性组合：

$$l = \sum_{i=1}^{3} l_i a_i = l_1 a_1 + l_2 a_2 + l_3 a_3,$$

其中 $l_i (i = 1, 2, 3)$ 应为正整数. 对于晶格，在平移变换 $T(l)$ 下，

$$r \rightarrow r' = T(l) = r + l,$$

具有不变性，所有$\{T(l)\}$集合构成基本平移群，或点阵的格群. 平移矢量$\boldsymbol{l}$的集合$\{\boldsymbol{l}\}$生成三维晶体点阵，即布拉菲点阵. 布氏点阵是基本平移操作的几何表现，晶格点阵则是晶格粒子的实际分布. 晶格点阵可以是一个布氏点阵，也可能由多个相同的布氏点阵套构而成. 例如 NaCl 的晶格点阵就是由氯离子和钠离子分别构成的面心立方布氏格子套构而成的.

2. 晶格的一般对称

将保持晶格不变性的所有对称操作记为$g(R,\alpha)$，

$$r \to r' = g(R,\alpha)r = Rr + \sum_{i=1}^{3}\alpha_i a_i,$$

其中R为$O(3)$变换，α_i为正实数，其整数部分为l_i，即

$$\alpha_i = l_i + t_i (0 \leqslant t_i \leqslant 1)(i = 1,2,3),$$

即$g(R,\alpha) = T(t)g(R,t)$.

当$\alpha = 0$时，$g(R,0)$表示转动与反射；当$R = E$，α_i必须取整数，表示平移变换，$g(E,l) = T(l)$，相继两次操作定义为它们的乘积，则

$$g(R,\alpha)g(R',\alpha') = g(R \cdot R', \alpha + R\alpha').$$

$g(R,\alpha)$的逆元素是$g(R^{-1}, -R^{-1}\alpha)$，而单位元素为$g(E,0)$，显然，所有晶格对称操作集合$\{g(R,\alpha)\}$满足群的四个公理. 这样构成的晶格对称群称为空间群，记为S. 上述晶格群$\{T(l)\}$，可以证明是群S的正规子群，其陪集元素可以表示为上式.

由于$g(R,t)$中的R与t有一一对应的关系，故平移群的陪集集合(包括平移群)与实$O(3)$的变换存在一一对应关系. 这样的$O(3)$群同构于商群$S/T(l)$，称为晶格点群，简称点群，记为G. 一般说来，集合$\{g(R,t)\}$并不构成群；点群亦非空间群的子群. 只有当$t = 0$，$g(R,0) = R$时，点群才是空间群的子群. 这种空间称为简单空间群.

3. 周期性条件对实正交变换 R 的限制

由于平移群元$T(l)$的共轭元$g(R,\alpha)^{-1}T(l)g(R,\alpha) = g(E,l') = T(l')$(其中$l' = Rl$)也是共轭元素，因此平移群是空间群的不变子群.

设$\{e_a\}$为正交归一基矢组，则有$e_a \cdot e_b \equiv \langle e_a, e_b \rangle = \delta_{ab}(a,b = 1,2,3)$. 实正交变换矩阵元$\Gamma(R)_{ab} = e_a \cdot Re_b \equiv \langle e_a, Re_b \rangle$. 转换以$\{a_i\}(i = 1,2,3)$为基矢组，且令$a_i = \sum_{a=1}^{3} e_a X_{ai}(i = 1,2,3)$，显然实矩阵$X$为正则的，即$\det X \neq 0$. 引入倒格基矢$b_i(i = 1,2,3)$，$b_i = \sum_{a=1}^{3}(X^{-1})_{ia}e_a$. 有

$$b_i \cdot a_j = \langle b_i, a_j \rangle = \langle \sum_{k=1}^{3}(X^{-1})_{ik}e_k, \sum_{l=1}^{3}e_l X_{lj} \rangle$$
$$= \sum_{k,l} X_{lj}X_{ik}^{-1} \langle e_k, e_l \rangle = \sum_k X_{ik}^{-1}X_{kj} = (X^{-1}X)_{ij} = \delta_{ij}.$$

以晶格基矢为基，实正交变换 R 的表示矩阵 $\overline{R}$ 一般不再是实正交的；其矩阵元 $\overline{R}_{ij}$ 为 $Ra_i = \sum_j a_j \overline{R}_{ji}, Rb_i = \sum_j \overline{(R^{-1})}_{ij} b_j$

$$\overline{R}_{ij} = \langle b_i, Ra_j \rangle = \langle a_j, R^{-1}b_i \rangle \Rightarrow \overline{R} = X^{-1}RX.$$

上式用并矢表示如下（省去 $\overline{R}$ 上一横）：

$$\overrightarrow{R} = \sum_{i,j} R_{ij}a_i \cdot b_j = \sum_{i,j}(R^{-1})_{ij}b_j \cdot a_i,$$

其中 $R_{ij} = b_i \cdot \overrightarrow{R} \cdot a_j = a_j \cdot (\overrightarrow{R}^{-1})b_i$，式中 $l_i' = R_{ij}l_j (i,j = 1,2,3)$，$R_{ij}$ 应为整数. 当然，其迹亦应为整数. 在等价相似变换中，矩阵的迹不变. 为不失一般性，以 Oz 为转轴，则相应的转动矩阵为

$$\Gamma(R) = \begin{bmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

即 $Tr[\Gamma(\varphi)] = 1 + 2\cos\varphi = \pm$ 整数，亦即 $\varphi = \frac{2\pi m}{n}, n = 1,2,3,4,6, m = 0,1,2,\cdots$.

对应 C_n 和 $S(n)$ $(\det\Gamma(R) = \pm 1)$ 分别叫 n 次固有和非固有循环点群. $S(n)$ 包括转动与反射元素. $S(1)$ 只有两个元素，空间反映 i 或 $\bar{i}$ 和恒元 E. $S(3)$ 的阶为 6. 其余循环点群的阶数均等于其次数减 n.

定理 5.3.1　除一次轴外，沿任一转轴方向必有晶格矢量或倒晶格矢量；在与转轴垂直的平面内，至少有两个不共线的晶格矢量和倒晶格矢量.

证明　除一次轴外，所有循环点群都包含 C_2、C_3 或 S_2. 易见，$C_2l + l$ 平行于转轴，$l - C_2l$ 则垂直于转轴（图 5.12）. 在此两矢量决定的平面以外找到任何晶格矢量 l'，则 $l' - C_2l'$ 为与 $\boldsymbol{n}$ 垂直，且与 $l - C_2l$ 线性无关的另一晶格矢量.

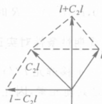


图 5.12　$l + C_2l$ 平行转轴，$l - C_2l$ 垂直转轴

对于 $S(2)$ 群，证法相同. 对于 C_3 群，则 $l + C_3^1l + C_3^2l$ 平行于转轴 n（直接作图易知），$l - C_3^1l - C_3^2l$ 垂直于转轴 $\boldsymbol{n}$. 对于倒格矢量 K，由于 $K \cdot l =$ 整数，而且

$$(RK) \cdot l = \sum_{i,j}(R_{ij}k_j)l_i = \sum_{i,j}k_jR_{ij}l_i$$
$$= \sum_{i,j}k_jR_{ji}^{-1}l_i = K \cdot (R^{-1}l),$$

亦即 RK 亦为倒晶格矢量. 因此可以利用上法，证明有关结果.

在晶体对称变换 $g(R,t)$ 中，往往有保持不变的点(不动点)、保持不变的直线和平面，分别称为对称中心、对称轴和对称平面. 对这些对称元的讨论，也有许多好的结果.

问题 5.3

1. 证明：平移群 $\{T(l)\}$ 是空间群 $\{g(R,\alpha)\}$ 的不变子群.

2. 证明：对于给定的晶格和选定的晶格基矢，$\forall\ g(R,t) \in S$，其中 R 与 t 有一一对应关系.

[提示：设 $g(R,t)$ 与 $g(R,t') \in S$，则 $g(R,t^{-1}) \cdot g(R,t') = T(-R^{-1}t + R^{-1}t') = T(l)$，即 $-R^{-1}t + R^{-1}t' = l \to t' - t = R_l = l' = 0$，即 $t' = t$. 注意 $\alpha = l + t, 0 \leqslant t_i \leqslant 1, i = 1,2,3$.]

3. 证明：若有 σ_v 面通过 C_n 轴，则 C_n 轴成为双向轴.

[提示：令 $\sigma_v = C_2 i$，C_2 垂直于 σ_v 面，也垂直于 C_n 轴，故

$$\sigma_v^{-1} C_n^k \sigma_v = i C_2 C_n^k C_2 i = i C_n^{-k} i = C_n^{-k}.]$$

4. 在直角坐标系中，写出转轴即 Oz 轴、n 次固有转动和非固有循环点群的生成元的矩阵形式和并矢形式，并计算 $\{\bar{3}\}$ 和 $\{\bar{4}\}$.

5. 用并矢计算绕[111]方向($n = \frac{1}{\sqrt{3}}i + \frac{1}{\sqrt{3}}j + \frac{1}{\sqrt{3}}k$)120°的矩阵.

§5.4　点　　群

第一类点群不包括反射元素，也称固点群. 固有循环点群 C_n，当 $n \geqslant 3$ 时称为高轴群. 第一类点群分类与高次轴关系极大.

1. 固有循环点群 C_n

C_n 群又称单轴点群. $\forall\ C_n^k \in C_n (k = 0,1,\cdots,n-1)$ 都相互对易，故 C_n 群为阿贝尔群. 其每个群元即为一个共轭类，有 n 个不等价不可约的一维表示. 在分子物理中，一般的线性链状分子，可用 $C_\infty (n \to \infty)$ 描述，即 C_∞ 中任一微小转动，分子构型依然重合，此时分子链的方向即转轴方向.

实际上，C_∞ 就是特殊正交群 $SO(2)$. 对于晶体对称群 S，由于周期性结构的限制，已经证明只可能存在 $n = 1,2,3,4,6$ 五种情况. 我们还给出各次转动轴的数目的关系 $n_2 = 3 + n_4 + 3n_6$(至少有两个轴不重合).

2. D_n 群

D_n 群即高次轴不多于一个的多轴点群. 此时群必包含 C_2，且 C_2 轴必垂直于 C_n 轴，

见图 5.13. 否则，如果是斜交，则

$$C_2C_n^kC_2 = C_n'^k,$$

必存在等价轴不属于所讨论的范围. 在 §6.1 及后面问题中已知，

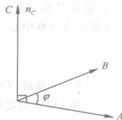


图 5.13

$$C_2(B)C_2(A) = C(c,2\varphi) \Rightarrow C_2(A) = C_2(B)C(c,2\varphi),$$

令 $C(c,2\varphi) = C_n^k(k=1,\cdots,n-1)$，即产生 $(n-1)$ 个 $C_2(A) = C_2(B)C_n^k$ 轴. 换言之，如图 5.14 所示，D 群即是由一条 C_n 轴、n 条 C_2 轴（均垂直于 C_n 轴）构成的第一类点群，其中 n 条 C_2 轴均垂直于 $\boldsymbol{n}$，可表为

$$C_2 = C_n^{-1}C_2^{(j)}C_n,$$

共有 $C_2^{(0)},C_2^{(1)},\cdots,C_2^{(n-1)}$，其中 $C_2^{(i)}$ 与 $C_2^{(j)}$ 表示任两个 C_2 轴. 相邻 C_2 轴夹角为 $\frac{2\pi}{n}$. C_n 轴由于有垂直于它的 n 个 C_2 轴，故应为双向轴. D_n 群共有 $2n$ 个元素.

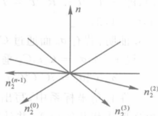


图 5.14

当 n 为奇数时，n 个 C_2 轴构成一组彼此等价的轴，即

$$\{C_2^{(1)},\cdots,C_2^{(n)}\} \equiv n\{C_2\}$$

构成一个共轭类. 当 n 为偶数时，n 个 C_2 轴分为两个共轭类. 由于 $\boldsymbol{n}$ 为双向轴，故 C_n^k 与 $C_n^{-k}(k=1,2,\cdots,(n-1)/2)$ 为一类.

当 n 为奇数时，$2n$ 个元素构成的 D_n 群，其共轭类个数为 $(n+3)/2$：

$$\{E\},\{C_2\},\{C_n^1,C_n^{(n-1)}\},\cdots,\{C_2^{(n-1)/2},C_2^{(n+1)/2}\},$$

元素个数　1　n　$\left(\frac{n-1}{2}\right)\times 2$　　总数 $=2n$

类　　数　1　1　$\frac{n-1}{2}$　　总数 $=\frac{n+3}{2}$

当 n 为偶数时，D_n 群有 $\frac{n+6}{2}$ 个共轭类：

$$\{E\},\{C_2\},\{C'_2\},\{C_n^1,C_n^{-1}\},\cdots,\{C_2^{(n-1)/2},C_2^{(n+1)/2}\},\{C_n^{n/2}\}$$

元素个数　1　$\frac{n}{2}$　$\frac{n}{2}$　$1+\left(\frac{n}{2}-1\right)\times 2=(n-2)+1=n-1$

类　　数　1　1　1　$\left(\frac{n}{2}-1\right)+1=\frac{n}{2}$

其中 $\{C_2\}$ 与 $\{C'_2\}$ 为两个不等价的二次转动.

在晶体点群中，D_n 的 $n=1,2,3,4,6$.

D_2 群，群元素为 4，有 2 个互相垂直的 C_2 与 C'_2 轴，它们生成第三个 C_2 轴 —— C''_2，

与C_2,C'_2均垂直:$C''_2 \perp C'_2$,$C''_2 \perp C_2$,它们构成4个元素构成的阿贝尔循环群(同构于空间反射群),$D_2 = (E, C_2, C'_2, C''_2)$. 该群有4个共轭类,即4个不等价不可约一维表示. 由$g = l_1^2 + l_2^2 l$ 得 $l_1 = l_2 = l_3 = l_4 = 1$.

D_3群,群元素$g = 6$,类为3. 有$l_1 = l_2 = 1$,$l_3 = 2$,此群同构于S_3群.

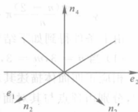


图 5.15 D_4 群转轴

D_4群,群元素$g = 8$,类为5. 如图5.15绕主轴$\boldsymbol{n}_4$转动,分两类$\{C_4^1, C_4^3\}$与$\{C_4^2\}$. 两组不等价二次轴C_2转动,分别构成$\{C_2\}$与$\{C_2^1\}$类. $\{C_2\}$组的转轴为$\boldsymbol{n}_2$,即$\boldsymbol{e}_1$方向,有两元素$C_2^{(1)}$与$C_2^{(2)}$(其中$C_2^{(2)}$为绕等价转轴$\boldsymbol{e}_2$转动π). $\{C_2^1\}$组的转轴为

$$n_2^1 = \frac{1}{\sqrt{2}}(e_1 + e_2),$$

包含$C_2^{1(1)}$与$C_2^{-1(2)}$. D_4群有4个一维、1个二维不等价不可约表示.

D_6群,有12个群元素,分6个共轭类:恒元,绕主轴$\boldsymbol{n}_6$转动的3类$\{C_6^1, C_6^5\}$、$\{C_6^2, C_6^4\}$、$\{C_6^3\}$,两组不等价的2次转动$\{C_6\}$、$\{C_6^1\}$,每组3个元素.

第一组$\{C_6\}$的转轴$\boldsymbol{n}(2)$为$\boldsymbol{e}_1$方向,第2组转轴为$\boldsymbol{n}'(2) = \frac{1}{2}(\sqrt{3}\,\boldsymbol{e}_1 + \boldsymbol{e}_2)$,与$\boldsymbol{e}_1$成30°角.

3. T、O和I点群

设除C_n轴以外,还存在其他的高次轴与C_n相交于一点O. 记C_m为与C_n轴夹角最小的高次轴. 由

$$C_m^{(k)} = C_n^{-k} C_m C_n^k (k = 1, 2, \cdots, n),$$

得到n个等价C_m轴围绕C_n轴,夹角相等. 以O为中心,任意半径的球面,连接n个C_m轴与球面的交点,得到球面内接正n边形,C_n轴则通过多边形中心.

显然在正多边形中再无其他转轴. 这个正n边形与n个等价C_m轴构成一个正多面体,同样在每个C_m轴边,也有夹角最小的m个等价的C_n轴,因此在每个C_m轴周围,亦可构成一个球内接正多面体,顶点就是C_m轴与球面的交点. 高次轴的点群正是描述这种球内接多面体对称性的点群. 实际上相应的点群只有几种.

例 5.4.1 $n = 3$,$m = 4$,构成球内接立方体. 每个顶角均为3面($n = 3$)正顶角,这3面中每一面都是正四边形.

一般说来,由相等的正n边形围成的正多面体,每个m面正顶角是凸顶角,则m个正多边形顶角的总和φ满足条件

$$\varphi = \frac{m(n-2)}{n}\pi < 2\pi(n,m \geqslant 3).$$

由上条件得到如下结果.

(1) 当 $n=3, m=3, \varphi=\pi<2\pi$,

相应正四面体描述其对称性的点群,记为 T. 该群有 4 个等价 3 次轴 $C_3^{(1)}$、$C_3^{(2)}$、$C_3^{(3)}$、$C_3^{(4)}$,分别由顶点与其对面中心连线得到. 它们应给出 9 个元素,$\{E, 4C_3^1, 4C_3^2\}$. 同时 4 个 C_2 轴的联合作用,得到 3 个 C_2 轴. T 群有 12 个元素,分 4 个共轭类,有 3 个一维表示和 1 个三维不可约表示.

(2) 当 $n=4, m=3, \varphi=\frac{3}{2}\pi<2\pi$,

相应立方体描述的对称点群记为 O. 注意连结正八面体各面心就得到正方体,两者具有相同的对称性. 以立方体而论,O 群元素应为 4(每面有 E, C_4^1, C_4^2, C_4^3) × 6 个面 = 24 个元素,群元分为 5 类:

$$E, 4(C_3^1, C_3^2), 3(C_4^1, C_4^3), 3(C_4^2 = C_2), 6(C_2),$$

其中 C_3 轴为立方体对角线,有 4 条;C_4 轴为相对面中点的连线(或沿相邻三条棱的方向),有 3 条;C_2 轴为沿立方体侧面的对角线方向,如 $\frac{1}{\sqrt{2}}(i+j)$ 等,有 6 条.

注意,等价的四次轴转动分为两类. 由 $1^2+1^2+2^2+3^2+3^2=24$ 可见,在 O 群的 5 个不等价不可约表示中,有 2 个一维表示,1 个二维表示和 2 个三维表示.

(3) 当 $n=3, m=4, \varphi=\frac{4}{3}\pi<2\pi$,

相应正八面体与正方体有完全相同的对称性. 实际上,正八面体亦可视为球内接正方体,其 6 个面心连结起来,即构成正八面体的 6 个正顶角,因此能使立方体重合的对称操作也能使正八面体重合;反之亦然. 结论就是正八面体相应的对称群依然是 O 群.

(4) 当 $n=5, m=3, \varphi=\frac{6}{5}\pi<2\pi$,

相应正五角十二面体,对称点群记为 I. 群元素为 60 个,分为 5 个类:

$$E; 10(C_3^1, C_3^2); 6(C_5^1, C_5^4); 6(C_5^2, C_5^3); 15(C_2).$$

其中 10 条等价 C_3 轴,为相对顶点的连线;6 条等价 C_5 轴,为相对正五边形面心的连线;15 条等价的 C_2 轴,则是相对棱中点的连线.

由 $1^2+3^2+3^2+4^2+5^2=60$ 可知,在 I 群的 5 个不等价不可约表示中,有 1 个一维表示,2 个三维表示,1 个四维表示和 1 个五维表示.

(5) 当 $n=3, m=5, \varphi=\frac{5}{3}\pi<2\pi$,

相应于正三角二十面体,将正五角十二面体的面心连结起来,就是正三角二十面

体. 显然，描述正二十面体对称性的点群亦为 I 群.

必须强调指出，在三种正多边体点群 T、O 和 I 中，只有 O 群和 T 群才是晶体点群，原因是 I 群包含有在晶体对称性中不存在的 C_5 轴. 但在描述分子对称性，如最近发现的 C_{60} 及其衍生物中，I 群却是十分重要的.

为便于了解有关对称操作和对称轴的详情，现将有关多面体的几何元素归纳于表 5.2 中，将有关固有点群群结构归纳于表 5.3 中.

表 5.2　高次轴点群相应多面体的几何结构

点群符号	名　称	表　面	顶角数	棱边数
T	正四面体	4 个正三角形	4	6
O	立方体	6 个正方形	8	12
O	正八面体	8 个正三角形	6	12
I	正五角十二面体	12 个正五角形	20	30
I	正三角二十面体	20 个正三角形	12	30

表 5.3　第一类点群结构简表

点群符号	阶	共轭类数	包括各转轴个数				不等价不可约表示的个数					分解为循环群的直积	生成元	指数为 α 的不变子群
			C_2	C_3	C_4	C_6	一维	二维	三维	四维	五维			
C_1	1	1					1					C_1	C_1	
C_2	2	2	1				2					C_2	C_2	
C_3	3	3		1			3					C_3	C_3	C_1
C_4	4	4			1		4					C_4	C_4	C_2
												C_5	C_5	
C_6	6	6				1	6					C_6	C_6	C_3
D_2	4	4	3				4					C_2, C'_2	C_2, C'_2	C_2
D_3	6	3	3	1			2	1				C_3, C'_2	C'_3, C''_2	C_3
D_4	8	5	4		1		4	1				C_4, C'_2	C'_2, C''_2	C_4, D_2
D_6	12	6	6			1	4	2				C_6, C'_2	C'_2, C''_2	C_6, D_3
T	12	4	3	4			3		1			C_3, C'_2, C_2	C_3, C_2	
O	24	5	6	4	3		2	1	2			C'_3, C_4, C''_2	C'_4, C''_2	T
I*	60	5	15	10		6	1		2	1	1			

* 其中 I 群不属晶体点群，表中还漏列 6 个 C_5 轴.

4. 第二类点群

第二类点群的表示矩阵的行列式值为 -1，就是包括反射元素的旋转点群. 基于第一类点群的结构分析，研究第二类点群的结构与分类.

我们已经知道 $O(3)/SO(3) = C_i$(反射群) $= (E, i)$，其中 E 为恒元，i 为反射操作.

$O(3) = SO(3) \otimes C_i = SO(3) \oplus iSO(3)$，其中 $SO(3)$ 即为固有（纯）转动群，i、$\{R(3)\}$ 则为 $O(3)$ 的正规子群 $SO(3)$ 的陪集，$SO(3)$ 为 $O(3)$ 的指数为 2 的正规子群，即第一类点群.

设 G 为第二类点群，将它如下分解 $G = H \cup iF, H \cap iF = \Phi$，其中集合 H 与 F 只包含正规（固有）转动.

(1) 当 $i \in G$ 时，第二类点群称为 I 型第二类点群.

由于 $H \subset G, F \subset G$，用 i 左乘 $G = H \cup iF, H \cap iF = \Phi$，则 $G = iH \cup F$，知 $H = F = SO(3), G = H \otimes C_i$，其中 H 为第一类点群，即 I 型第二类点群由第一类点群与反射群的直积构成，其不可约表示为第一类点群与 C_i 群不可约表示的直积.

(i)$n =$ 偶数. $C_{nh} = C_n \otimes C_i, D_{nh} = D_n \otimes C_i$. 对于晶体点群，$n = 2,4,6$，下标 h 表示有垂直于偶次轴的反射面. 第二类点群的群元素是相应第一类点群的 2 倍.

(ii)$n =$ 奇数. $S_{2n} = G_n \otimes C_i, D_{nd} = D_n \otimes C_i$. 对于晶体点群，$n = 1,3$. 其中 $n = 1$，对应的 $C_{2i} \equiv S_2 = \{E, i\}, D_d = \{E, \sigma\}$，这里 d 表示群中包含通过主轴（或 $\boldsymbol{k}$ 轴）的平面的反射. 这两个点群不包含主轴，称为无轴点群. 当 $n = 3$ 时，$S_{23} \equiv C_{3i} = C_3 \otimes C_i, D_{3d} = D_3 \otimes C_i$，元素比相应第一类点群增加一倍，即 $2n$ 个.

(iii) 第二类多面体点群，$T_h = T \otimes C_i, O_h = O \otimes C_i$，若不限于晶体群，还有 $I_h = I \otimes C_i$. T_h 群的对称性可以用图 5.16 所示立方体表示. 其中 σ_h 面平分 4 个 C_3 轴. 3 个等价的 σ_h 面都通过正方体中心，且垂直于 3 个 C_2 轴. 有 24 个群元素. O_h 群的对称性可以用图 5.17 所示立方体来表示. 注意其中 σ_d 与 σ_h 与 T_h 的异同. 此时 3 个 C_4 轴取代 T 群的 3 个 C_2 轴. T_h 群有 48 个元素.

I_h 群为晶体点群以外的点群. 以与 O_h 群相似的方法引入 σ 面，共有 120 个元素. 其不可约的最高维为五维.

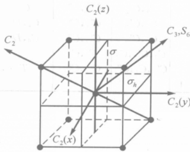


图 5.16　T_h 对称性

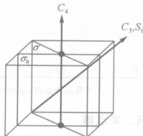


图 5.17　O_h 对称性

(2) 当 $i \notin G$ 时，相应点群称为 p 型第二类点群. 可以证明（见问题 3），其构造方法

是从第一类点群 M 出发，遍取所有阶数为其一半的所有子群 H，按如下方式构造 $G = H \cup i(M-H)$，即可得到 p 型点群：

$$S_{2n} = C_n \cup i(C_{2n} - C_n) = C_n \cup iC'_{2n}C_n, n = \text{偶数},$$
$$C_{2h} = C_n \cup i(C_{2n} - C_n) = C_n \cup iC'_{2n}C_n, n = \text{奇数},$$
$$C_{nv} = D_n \cup i(D_{2n} - D_n) = D_n \cup \sigma_v C_n, n = 2,3,\cdots,$$
$$C_{nd} = D_n \cup i(D_{2n} - D_n) = D_n \cup iC'_{2n}D_n, n = \text{偶数},$$
$$T_d = T \cup i(O - T) = T \cup iC'_4 T,$$

其中 C_{nv} 群中，反映面 $\sigma''C_n$ 轴，且通过 C_n 轴，$C_{nv} \in \sigma_v, C_n^k \in C_{nv} (k = 1, \cdots, n-1)$.

可以证明，C_{nv} 与 D_n 同构(见问题 4)；T_d 群的对称性可见图 5.18.

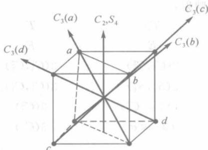


图 5.18　T_{dh} 对称性

其中 T 群的 4 个顶角为 a、b、c、d，4 条立方体对角线就是 C_3 轴，3 条对面中心连线就是 C_2 轴. 可以证明，T_d 群同构于 O 群. 其他符号的意义，前文均已交代清楚.

总之，p 型第二类点群与相应的第一类点群同构. 实际上，由前者可以构造后者，由后者亦可构造前者，即将第一类点群的任一指数为 2 的正规子群作为固有子群，然后将其陪集元素分别乘以 i，即得到非固有转动，由此可以得到与原来 p 型第二类点群同构的第一类点群.

习题 5.4

1. 在直角坐标系中表示出

(1) D_3 群所包含的所有转轴的方向.

(2) O 群各转轴的方向，并指出构成其子群 T 的转动变换.

2. 证明：T 群的所有元素都可以唯一表示为子群 C_3^1 和 D_2 的对应元素之积.

3. 证明：对开定理，即 $G = H \cup i(M-H)$.

[提示：在 $G = H \cup iF, H \cap iF = \Phi$ 中，应有 $H \cap iF = \varnothing$；否则，$\forall g \in H \cap$

$iF \Rightarrow ig \in iF \subset G \Rightarrow igg^{-1} = i \in G$. 设 $\forall\ h_i \in H$,有 $\det \Gamma(h_i) = +1$,H 为 G 的子群,其阶设为 n_h. 设 $\forall\ f_\alpha, f_\beta \in F$,由 $h_i, ih_\alpha \in G \Rightarrow h_i h_\alpha \in F$,$h_\alpha h_i \in F$. 令 h_i 遍及 H,则 $n_h \leqslant n_f$(F 集合元素个数). 又由 $if_\alpha \cdot f_\beta = f_\alpha f_\beta \in G$,且 $f_\alpha f_\beta \in H$,此式对 F 中所有元素成立 $\Rightarrow n_f \leqslant n_h$. 所以 $n_h = n_f$. 设 $M = H \cup F$,由 $h_i f_\alpha \in F \subset M$,$h_i h_j \subset H$ 及 $f_\alpha f_\beta \in H \subset M$,故知 M 为群,且为第一类点群,不含 i,故不同于 G. 于是 $F = M - H$.]

4. 证明:C_{nv} 同构于 D_n 群.

[提示:只要有一个 σ_v 通过 C_n 轴,必有 n 个 σ_v 面通过 C_n 轴,且 C_n 轴变为双向轴 $\Rightarrow C_n^k$ 与 C_n^{-k} 同类. n 为奇数时,与 D_n 轴 C_2 轴一样,n 个 σ_v 面属于同一类.

n 为偶数时,n 个 σ_v 面分为两个等价类. 于是 $C_{n\sigma}$ 群中 n 个 σ_v 操作与 D_n 群的 n 个 C_2 轴操作可以建立一对应的映射:

	T_d	T
1 类	E	E
2 类	$3(C_3^1, C_3^2)$	$3(C_3^1, C_3^2)$
3 类	$3(S_4^1, S_4^3)$	$3(C_4^1, C_4^3)$
4 类	$3(S_4^2 = C_4^2)$	$3(C_4^2)$
5 类	$6\sigma_2 \equiv \sigma$	$6(C_2)$

5. 证明:$S_n \cong C_{nh}$.

[提示:$S_n = C_n \sigma_h$,$n = 1,2$,即无轴第二类点群. $n \geqslant 3$,由 $(S_n)^n = C_n^n \cdot \sigma_h = \sigma_h \in G$,由 $C_2^1 \in G$,$C_n^k \in G \Rightarrow S_n = C_{nh}$. 当 $n =$ 偶数时,σ_h 与 C' $(C' = \sigma C_n^k \sigma)$,等价于 C 有 $(C_n^1 \sigma_h)^2 \in G \Rightarrow C_n^2 = C'_{n/2} \in G$,即 S_{2n} 的像转轴包含了 C_n 的正规转轴. 当 n 为偶数时,$S_n^n = C_n^n \sigma_h^n = E$,为 n 阶循环群;当 n 为奇数时,$S_n^n = C_n^n \sigma_h^n = \sigma_h \neq E$,为 $2n$ 阶循环群. $S_n \cong C_n \sigma_h$.]

6. 试证:$T_d \cong O$ 群.

7. 设 G 为多面体群,利用对开定理,构造 p 型第二类点群.

[提示:T 群与 I 群无指数为 2 的子群. O 群令 $H = T$,则 $O - T = C_4^1 T$,即 $O = T \oplus C_4^1 T$,第二类点群 $M = T \oplus iC_4^1 T$.]

8. 设 $G = C_{2n}$,利用对开定理构造 M.

[提示:令 $H = \{E, C_{2n}^2, \cdots, C_{2n}^{2n-2}\} = C_n$,则 $G - H = C_{2n} - C_n = C_{2n}^1 \cdot C_n$,故 $M = C_n \oplus iC_{2n}^1 C_n$,当 n 为偶数时,$M = S_n$;当 n 为奇数时,$M = C_{nh}$.]

§5.5 晶体点群

晶体的结构的平移不变性,限制只有 $n = 1,2,3,4,6$ 次转轴(主轴和像转轴),结果

使得晶体点群只有 32 种，分为 7 大系列.

在 §5.3 节，我们知道晶格矢量可以表为 $l = \sum_{i=1}^{3} l_i a_i = l_1 a_1 + l_2 a_2 + l_3 a_3$，

晶体中任意位矢 $\boldsymbol{r}$，在所谓基本平移 $\boldsymbol{r} \to \boldsymbol{r} + \boldsymbol{l}$ 下，晶体结构具有不变性，且 $\{l_1, l_2, l_3\}$ 集合生成布拉菲点阵，$\boldsymbol{l}$ 称格矢. 晶体点群是晶格的布拉菲点群的对称群，它可以描述晶格点阵的对称性、宏观对称性，但一般说来并不是晶体点阵本身的对称群.

试考虑布拉菲格子(图 5.19)，七种晶系如下：

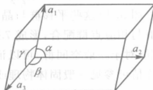


图 5.19

(1) 三斜系. 布氏格子中，$\boldsymbol{a}_1 \neq \boldsymbol{a}_2 \neq \boldsymbol{a}_3$，且 $\alpha \neq \beta \neq \gamma$. 相应点群 C_1 和 C_i 只有简单三斜系(P)一种.

(2) 单斜系. $\boldsymbol{a}_1 \neq \boldsymbol{a}_2 \neq \boldsymbol{a}_3$，但 $\alpha \neq \frac{\pi}{2}, \beta = \gamma = \frac{\pi}{2}$(正交). 相应点群 C_2、C_{2h} 和 $C_s = \{E, \sigma\}$. 除简单单斜式(p)外，还在上、下面心有点阵，称底心单斜晶体(C).

(3) 正交系. $\boldsymbol{a}_1 \neq \boldsymbol{a}_2 \neq \boldsymbol{a}_3, \alpha = \beta = \gamma = \frac{\pi}{2}$，对应点群 $D_{2h}(8)$(这里 8 表示包含 8 个元素，下同)、$D_2(4)$ 和 $C_{2v}(4)$. 正交系又包括简单正交(P)、底心正交(C)、体心正交(I)和面心正交(F)等. 对于 C_2，还有侧心正交(A).

(4) 三方系. $\boldsymbol{a}_1 = \boldsymbol{a}_2 = \boldsymbol{a}_3$，且 $\alpha = \beta = \gamma = \frac{2}{3}\pi$，对应点群 $C_3(3)$、$C_{3v}(6)$、$D_3(6)$、$D_{3h}(12)$ 和 $S_6(6)$. 只有简单三方(R)一种.

(5) 四方系. $\boldsymbol{a}_1 = \boldsymbol{a}_2 \neq \boldsymbol{a}_3$. $\alpha = \beta = \gamma = \frac{\pi}{2}$，有简单四方($P$)与体心四方($I$)两种. 对应点群 $C_4(4)$、$C_{4v}(8)$、$D_4(8)$、$D_{4h}(16)$、$C_{4v}(8)$、$D_{2d}(8)$ 和 $S_4(4)$.

(6) 六方系. $\boldsymbol{a}_1 = \boldsymbol{a}_2 \neq \boldsymbol{a}_3$，且 $\alpha = \beta = \frac{\pi}{2}, \gamma = \frac{\pi}{3}$，对应点群 $C_6(6)$、$C_{6h}(12)$、$C_{6v}(12)$、$C_{3h}(6)$、$D_6(12)$、$D_{6h}(24)$、$C_{3d}(12)$，只有简单六方(P)一种.

(7) 立方系. $\boldsymbol{a}_1 = \boldsymbol{a}_2 = \boldsymbol{a}_3$，且 $\alpha = \beta = \gamma = \frac{\pi}{2}$，对应点群 $T(12)$、$T_h(24)$、$T_d(24)$、$O(24)$ 和 $O_h(48)$，包括简单立方(P)、体心立方(I)、面心立方(F).

全部七种晶系具体结构见图 5.20，细分又有 14 类，其中包括 32 种点群.

图 5.20 中符号 P、I、A 与 F 等的含义是不同平移. 相应的平移变换记作 $\Gamma_{\frac{1}{2},\frac{1}{2},\frac{1}{2}}$，这样变换构成的平移群记为 T_l. 整个平移群记为 T_L. T_l 是 T_L 的不变子群. 根据 Γ 形式，将平移群分为以下四种类型：

(1)P：原始平移群，

$$T_L = T_L.$$

(2)I:体心平移群,

$$T_L = T_l\{E,\Gamma_{\frac{1}{2},\frac{1}{2},\frac{1}{2}}\}.$$

(3)A、B 和 C:底心平移群:

$$A:T_L = T_l\{E,\Gamma_{0,\frac{1}{2},\frac{1}{2}}\},B:T_L = T_l\{E,\Gamma_{\frac{1}{2},0,\frac{1}{2}}\},C:T_L = T_l\{E,\Gamma_{\frac{1}{2},\frac{1}{2},0}\}.$$

(4)F:面心平移群,

$$T_L = T_l\{E,\Gamma_{0,\frac{1}{2},\frac{1}{2}},\Gamma_{\frac{1}{2},0,\frac{1}{2}},\Gamma_{\frac{1}{2},\frac{1}{2},0}\}.$$

图 5.20 这些平移群与晶系结合起来,形成 14 种晶格类型,或布拉菲格子. 这些平移群与相应点群配合,形成 73 种简单空间群. 所谓简单空间群,系指点群是其子群的空间群. 对于一般空间群,可以证明,共有 230 种,它描述了所有可能的晶体的对称结构. 其详情可参见一般固体物理或晶体结构的书籍.

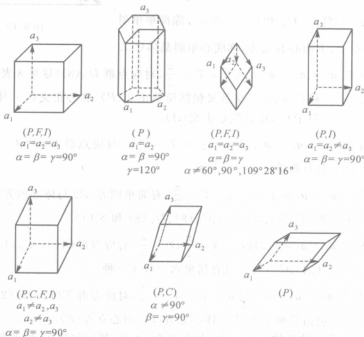


图 5.20　七种晶系结构(14 类结构说明)

表 5.4 列出 32 种点群的结构,图 5.20 列出了 14 种布拉菲格子基矢的配置,我们可以直观了解其几何结构. 在表 5.5 中则列出 32 种点群的特征标,以备查阅.

表 5.4　32 种点群结构

固有点群			非固有点群			
点群	分解为循环群的乘积	指数为二的不变子群	P 型(不含 I) 点群	P 型 循环群乘积	I 型(含 I) 点群	I 型 循环群乘积
C_1	C_1				C_i	C_1
C_2	C_2	C_1	C_1	C_s	C_{2h}	C_iC_2
C_3	C_3				C_{3i}	C_{3i}
C_4	C_4	C_2	S_4	S_4	C_{4h}	C_iC_4
C_6	C_6	C_3	C_{3h}	C_{3h}	C_{6h}	C_iC_6
D_2	$C_2C'_2$	C_2	C_{2v}	$C_2C'_s$	D_{2h}	$C_iC_2C'_2$
D_3	$C_2C'_2$	C_3	C_{3v}	$C_3C'_s$	D_{3d}	$C_{3i}C'_2$
		C_4	C_{4v}	$C_4C'_s$		
D_4	$C_4C'_2$	D_2	$D_{2d}(V_d)$	$S_4C'_2$	D_{4h}	$C_iC_4C'_2$
		C_6	C_{6v}	$C_6C'_s$		
		D_3	D_{3h}	$C_{3h}C'_2$	D_{6h}	$C_iC_6C'_2$
D_6	$C_6C'_2$					
T	$C'_3C'_2C'_2$				T_h	$C'_{3i}C_2C'_2$
O	$C'_3C'_4C''_2$	T	T_d	$C'_3S_4C''_s$	O_h	$C'_{3i}C_4C''_2$

表 5.5　32 种点群特征标

C_2	E	C_2
C_i	E	I
C_s	E	σ
χ^1	1	1
χ^2	1	-1

C_3	E	C_3	C_3^2
χ^1	1	1	1
χ^2	1	ε	ε^2
χ^3	1	ε^2	ε

$\varepsilon = \exp(-2\pi i/3)$

C_4	E	C_4	$C_4^{2'}$	C_4^3
S_4	E	S_4	$S_4^{2'}$	S_4^3
χ^1	1	1	1	1
χ^2	1	i	-1	$-$i
χ^3	1	-1	1	-1
χ^4	1	$-$i	-1	i

C_6	E	C_6	$C_6^{2'}$	C_6^3	C_6^4	C_6^5
C_{3h}	E	S_6	$S_6^{2'}$	S_6^3	S_6^4	S_6^5
χ^1	1	1	1	1	1	1
χ^2	1	ω	ω^2	-1	$-\omega$	$-\omega^2$
χ^3	1	ω^2	$-\omega$	1	ω^2	$-\omega$
χ^4	1	-1	1	-1	1	-1
χ^5	1	$-\omega$	ω^2	1	$-\omega$	ω^2
χ^6	1	$-\omega^2$	$-\omega$	-1	ω^2	ω

$\omega = \exp(-i2\pi/6)$

D_2	E	C_2	C'_2	C''_2
C_{2v}	E	C_2	C'_s	C''_s
C_{2h}	E	C_2	C_s	I
χ^1	1	1	1	1
χ^2	1	-1	1	-1
χ^3	1	1	-1	-1
χ^4	1	-1	-1	1

D_3	E	$C_3(2)$	$C'_2(3)$
C_{3v}	E	$C_3(2)$	$C'_s(3)$
χ^1	1	1	1
χ^2	1	1	-1
χ^3	2	-1	0

C_1	E
χ^1	1

D_4	E	C_4^2	$C_4(2)$	$C'_2(2)$	$C''_2(2)$
D_{4v}	E	C_4^2	$C_4(2)$	$C'_s(2)$	$C''_s(2)$
D_{2d}	E	S_4^2	$S_4(2)$	$C'_2(2)$	$C''_s(2)$
χ^1	1	1	1	1	1
χ^2	1	1	1	−1	−1
χ^3	1	1	−1	1	−1
χ^4	1	1	−1	−1	1
χ^5	2	−2	0	0	0

D_6	E	C_6^3	$C_6^2(2)$	$C_6(2)$	$C'_2(3)$	$C''_2(3)$
C_{6v}	E	C_6^3	$C_6^2(2)$	$C_6(2)$	$C'_s(3)$	$C''_s(3)$
D_{3h}	E	C_s	$S_6^2(2)$	$S_6(2)$	$C'_2(3)$	$C''_s(3)$
χ^1	1	1	1	1	1	1
χ^2	1	1	1	1	−1	−1
χ^3	1	−1	1	−1	1	−1
χ^4	1	−1	1	−1	−1	1
χ^5	2	2	−1	−1	0	0
χ^6	2	−2	−1	1	0	0

T	E	$C_2(3)$	$C_3(4)$	$C_3^2(4)$
χ^1	1	1	1	1
χ^2	1	1	ε	ε^2
χ^3	1	1	ε^2	ε
χ^4	ε	−1	0	0

$\varepsilon = \exp(-\mathrm{i}2\pi/3)$

O	E	$C_3(8)$	$C_4^2(3)$	$C''_2(6)$	$C_4(6)$
T_σ	E	$C_3(8)$	$S_4^2(3)$	$C''_2(6)$	$S_4(6)$
χ^1	1	1	1	1	1
χ^2	1		1	−1	−1
χ^3	2	−1	2	0	0
χ^4	3	0	−1	1	−1
χ^5	3	0	−1	−1	ε_1

晶体结构对称性决定晶体的物理性质，因此晶体点群、空间群有许多重要应用.

例 5.5.1　证明：立方晶系的介电常数为标量.

设介电常数张量为 $\varepsilon_{\alpha\beta}(\alpha,\beta = 1,2,3,$ 即 $x,y,z)$，则一般应有

$$D_\alpha = \sum_{\beta=1}^{3} \varepsilon_{\alpha\beta} E_\beta.$$

不失一般性，选择坐标，使 $E = Ej$（沿 y 轴），则

$$D_\alpha = \sum_{\alpha,\beta} \varepsilon_{\alpha\beta} E \delta_{\beta 2} = \varepsilon_{\alpha 2} E \equiv E_{\alpha y} E (\alpha = x,y,z).$$

以 y 轴为转轴，作 C_4^1 操作：$z \to z' = x, x \to x' = -z$，故 $D'_x = D_z, D'_z = -D_x$. 由于 C_4 不变性，应有 $D'_x = D_x, D'_z = D_z$，由此推知

$$\varepsilon_{xy} = \varepsilon_{zy} \text{ 和 } \varepsilon_{xy} = -\varepsilon_{zy} \Rightarrow \varepsilon_{xy} = \varepsilon_{zy} = 0.$$

再使外场 E 沿 z 轴和 x 轴方向作类似分析，可知 $\varepsilon_{xz} = \varepsilon_{yz} = \varepsilon_{yx} = \varepsilon_{zx} = 0$，即 $\varepsilon_{\alpha\beta}$ 所有非对角元素为零.

取 E 沿立方体对角线（C_3 轴），则给出

$$E_x = E_y = E_z = \frac{1}{\sqrt{3}} E, D_x = \frac{1}{\sqrt{3}} \varepsilon_{xx} E, D_y = \frac{1}{\sqrt{3}} \varepsilon_{yy} E, D_z = \frac{1}{\sqrt{3}} \varepsilon_{zz} E.$$

作 C_3^1 和 C_3^2 操作，并计及 C_3 不变性，即

$$D'_x = D_y, D''_x = D_z, D_x = D'_x = D''_x \Rightarrow D_x = D_y = D_z,$$

即 $\varepsilon_{xx} = \varepsilon_{yy} = \varepsilon_{zz} = \varepsilon$.

例 5.5.2　求 O 群的特征标.

O 群有24个元素，6个2次轴，4个3次轴，3个4次轴. O 群的5个类记为 I、$6C_2$、$8C_3$、$6C_4$、$3C_4$. 5个不等价不可约表示的维数由 $\sum_{i=1}^{5} l_i^2 = 24$ 得 $l_1 = l_2 = 1, l_3 = 2, l_4 = l_5 = 3$. $\{\chi_k^{(i)}\}$ 中，$\chi_k^{(i)} = l_k(k = 1,2,3,4,5)$，且 $\chi_1^{(i)}(E) = 1(i = 1,2,3,4,5)$，即特征标表第一行第一列已经算出.

注意关系，

$$C_2^2 = E \Rightarrow [\chi_2^{(2)}(C_2)]^2 = \chi_1^{(2)}(E) = 1, \text{得 } \chi_2^{(2)}(C_2) = \pm 1,$$

$$C_3^3 = E \Rightarrow [\chi_3^{(2)}(C_3^1) = 1]^2 = 1 \Rightarrow \chi_3^{(3)} = 1, \mathrm{e}^{\pm 2\pi i/3}.$$

$$C_4^2 \cdot C_3 = C_3^1 \Rightarrow \chi_4^{(3)}(C_4^2)\chi_3^{(2)}(C_3^1) = \chi_3^{(2)}(C_3^1)$$
$$\Rightarrow \chi^{(2)}(C_4^2) = [\chi_4^{(2)}(C_4)]^2 = 1.$$

由于 $\sum_{k=1}^{5} \chi_k^{(1)}\chi_k^{(2)} = 0$，有

$$\chi_3^{(2)}(C_3) = 1, \chi_2^{(2)}(C_2) = -1, \chi_4^{(2)}(C_4^1) = 1.$$

由于 $\sum_{k=1}^{5} \chi_k^{(1)} \cdot \chi_k^{(3)} = 0$, $\sum_{k=1}^{5} \chi_k^{(2)}\chi_k^{(3)} = 0$.

将两式相加、相减分别得

$$2 + 8\chi_3^{(3)}(C_3^1) + 3\chi_5^{(3)}(C_4^2) = 0, \chi_2^{(3)}(C_2^1) + \chi_4^{(3)}(C_4^1) = 0,$$

即
$$\chi_3^{(3)}(C_3^1) = -\frac{1}{4} - \frac{3}{8}\chi^3(C_4^2), \chi_4^{(3)}(C_4^1) = -\chi_2^{(3)}(C_2^1).$$

代入 $(\chi^{(3)}, \chi^{(3)}) = g = 24$，经整理有

$$12[\chi_2^{(3)}(C_2)]^2 + \frac{1}{2}[1 + \frac{3}{2}\chi_4^{(3)}(C_4^2)]^2 + 3[\chi_5^{(2)}(C_4^2)]^2.$$

但由于 $C_2^2 = I, C_4^4 = I$，得

$$\chi_2^{(3)}(C_2^1) = 0, \pm 2, \chi_5^{(2)}(C_4^2) = 0, \pm 2 \quad \text{(二维表示)}.$$

又由前面方程的约束，给出 $\chi_3^{(3)}(C_2^1) = 0, \chi_5^{(3)}(C_4^2) = 2$. 由此又定出

$$\chi_3^{(3)}(C_3^1) = -1, \chi_4^{(3)}(C_4^1) = 0.$$

再计算三维表示. 由

$$\sum_{k=1}^{5} \chi_k^{(1)} \cdot \chi_k^{(4)} = 0, \sum_{k=1}^{5} \chi_k^{(2)} \cdot \chi_k^{(4)} = 0,$$

$$\sum_{k=1}^{5} \chi_k^{(3)} \cdot \chi_k^{(4)} = 0, \sum_{k=1}^{5} \chi_k^{(4)} \cdot \chi_k^{(4)} = g = 24,$$

得

$$3+8\chi_3^{(4)}(C_3^1)+3\chi_5^{(4)}(C_4^2)=0,$$
$$\chi_2^{(4)}(C_2^1)+\chi_4^{(4)}(C_4^1)=0,$$
$$3+4\chi_3^{(4)}(C_3^1)+3\chi_5^{(4)}(C_4^2)=0,$$
$$9+12[\chi_2^{(4)}(C_2^1)]^2+3=24,$$

得

$$\begin{cases}\chi_3^{(4)}(C_3^1)=0,\\ \chi_5^{(4)}(C_4^2)=-1,\\ \chi_4^{(4)}(C_4^1)=-\chi_2^{(4)}(C_2^1).\end{cases}$$

因而，$\chi_2^{(4)}(C_2)=\pm 1$（正好对应两个三维表示）.

O 群特征标表见表 5.6 所示。

表 5.6　O 群特征标表 $\chi_k^{(i)}$

不可约表示(i) \ 类(k)	1 $\{E\}$	2 $\{6C_2^1\}$	3 $\{8C_3^1\}$	4 $\{6C_4^1\}$	5 $\{3C_4^2\}$
$\chi^{(1)}$	1	1	1	1	1
$\chi^{(2)}$	1	-1	1	-1	1
$\chi^{(3)}$	2	0	-1	0	2
$\chi^{(4)}$	3	-1	0	1	-1
$\chi^{(5)}$	3	1	0	-1	-1

问题 5.5

1. 计算群 $O_h=O\otimes C_i$ 的特征标表.

[提示见表 5.7]

2. 求出 O 群的所有不等价不可约表示.

[提示：两个一维表示即例 5.5.2 所给出的特征标. 取 O 的正规子群 $N=\{I,3C_4^2\}$，其商群 O/N 的阶数 $=6$，且 $O/N=\{N,C'_2N,C''_2N,C'''_2N,\ C_3N,C_3^2N\}$，$D_3=\{E,C'_2,C''_2,C'''_2,C_3,C_3^2\}$. 就是由群 O 到子群 D_3 的同态映射，$\forall\ g\in D_3,\forall\ gN\in O,gN\rightarrow g(4\rightarrow 1)$.

我们试由 D_3 的不可约表示，通过同态映射，构造 O 群的不可约表示. O 的生成元可取 C_3 和 C_2，其中 C_2 轴与 C_3 轴相邻. 由于 $C_2=C_4^{-2}C_2^1C_4^2$，有 O 群的二维表示

$$\Gamma^{(3)}(C_2)=\Gamma^{(3)}(C_4^{-2})\Gamma^{(3)}(C_2^1)\cdot\Gamma^{(3)}(C_4^2).$$

表 5.7　群 O_h 的特征标表

类 (k) 表示 (i)	1 E	2 $6C_2$	3 $8C_3$	4 $6C_4$	5 $3C_4^2$	6 i	7 $6iC_2$	8 $8iC_3$	9 $6iC_4$	10 $3iC_4^2$
$\chi^{(1)}$	1	1	1	1	1	1	1	1	1	1
$\chi^{(2)}$	1	1	1	1	1	−1	−1	−1	−1	−1
$\chi^{(3)}$	1	−1	1	−1	1	1	−1	1	−1	1
$\chi^{(4)}$	1	−1	1	−1	1	−1	1	−1	1	−1
$\chi^{(5)}$	2	0	−1	0	2	2	0	−1	0	2
$\chi^{(6)}$	2	0	−1	0	+2	−2	0	+1	0	−2
$\chi^{(7)}$	3	−1	0	1	−1	3	−1	0	1	−1
$\chi^{(8)}$	3	−1	0	1	−1	−3	1	0	−1	1
$\chi^{(9)}$	3	1	0	−1	−1	3	1	0	−1	−1
$\chi^{(10)}$	3	1	0	−1	−1	−3	−1	0	1	1

[提示：利用 $\chi(O_h)=\chi(0)\chi(C_i)$. 实际上所有第二类点群均可用此法得到.]

考虑到同态映射 $\Gamma^{(3)}(C_4^2)=E=\Gamma^{(3)}(C_4^{-2})$. 但 $D_3\cong C_{3v}$，其二维表示

$$\Gamma^{(3)}(C_2^1)=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ \Gamma^{(3)}(C_3^1)=\begin{bmatrix}-\dfrac{1}{2} & -\dfrac{\sqrt{3}}{2}\\ \dfrac{\sqrt{3}}{2} & -\dfrac{1}{2}\end{bmatrix}.$$

O 群的三维表示由自然基可得. 自然表示是不可约的，取 C_2 轴为角 $O\text{-}y\text{-}z$ 平分线，C_3 轴为 $O\text{-}x\text{-}y$ 的平分线，易得

$$\Gamma^{(4)}(C_2^1)=\begin{bmatrix}-1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{bmatrix},\Gamma^{(4)}(C_3^1)=\begin{bmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}.$$

至于另一个三维表示，可由特征标表 $\chi^{(5)}=\chi^{(2)}\chi^{(4)}$ 得到 $\Gamma^{(5)}=\chi^{(2)}$. $\Gamma^{(2)}$ 生成元矩阵

$$\Gamma^{(5)}(C_2^1)=\begin{bmatrix}1 & 0 & 0\\ 0 & 0 & -1\\ 0 & -1 & 0\end{bmatrix},\ \Gamma^{(5)}(C_3^1)=\begin{bmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{bmatrix}.$$

原则上所有点群的表示均可用此法得到.]

3. 求出 O_h 群的所有不等价不可约表示.

4. 设 $\hat{u}\equiv\hat{L}^2/\hbar$为哈密顿算符中与角度相关部分，有

$$\hat{u}Y_{lm}(\theta,\varphi)=l(l+1)Y_{lm}(\theta,\varphi),$$

其中 $Y_{lm}(\theta,\varphi)$ 为球谐函数，$l=0,1,2,\cdots;m=-l,\cdots,-1,0,1,\cdots,l$. $Y_{lm}(\theta,\varphi)$ 实际上为 $SO(3)$ 群不可约表示 $\{\Gamma^{(l)}(g)\}$ 的 $2l+1$ 个正交归一基矢. 请将 $\{\Gamma^{(l)}(g)\}$ 按 D_3 群约化.

[提示：在晶体场中，离子谱项分裂问题广泛碰到此类约化问题.

$$[\Gamma^{(l)}(g_a)]_{\mu\nu}=\mathrm{e}^{\mathrm{i}(l+1-\mu)}\cdot\delta_{\mu\nu}(\mu,\nu=1,2,\cdots,2l+1),$$

故特征标

$$\chi^{(l)}(g_a)=\sum_{m=-l}^{l}\mathrm{e}^{\mathrm{i}m\alpha}=\mathrm{e}^{-\mathrm{i}l\alpha}\cdot\sum_{k=0}^{2l}(\mathrm{e}^{\mathrm{i}\alpha})^k$$

$$=\mathrm{e}^{-\mathrm{i}l\alpha}\cdot\frac{\mathrm{e}^{\mathrm{i}(2e+1)\alpha}-1}{\mathrm{e}^{\mathrm{i}\alpha}-1}=\frac{\sin(l+\frac{1}{2})\alpha}{\sin\frac{1}{2}\alpha}.$$

对于 D_3：$E\Rightarrow\alpha=2\pi,\chi^{(l)}(2\pi)=2l+1$；

$$C_2(3)\Rightarrow\alpha=\pi,\chi^{(l)}(\pi)=\sin(\frac{\pi}{2}+l\pi)=\begin{cases}-1 & (l\text{ 为奇数}),\\ +1 & (l\text{ 为偶数}),\end{cases}$$

$$C_3(2)\Rightarrow\alpha=\pm\frac{2}{3}\pi,$$

$$\chi^{(l)}(\pm\frac{2}{3}\pi)=\frac{\sin(\pm\frac{2\pi l}{3}\pm\frac{\pi}{3})}{\sin(\pm\frac{2}{3}\pi)}=\begin{cases}l, & l=3m,\\ 0, & l=3m+1,\\ -1, & l=3m-1.\end{cases}$$

总结这些结果，即得表 5.8. 其中 Γ_1、Γ_2 与 Γ_3 为 $\Gamma^{(l)}(g)$ 的 2 个一维表示和 1 个二维表示，而 a_1、a_2 与 e 则为 D_3 的 2 个一维表示与 1 个二维表示. $\{\Gamma^{(l)}(g_a)\}$ 实际上有无穷多个不可约表示. $SO(3)$ 是连续群.

表 5.8　$SO(3)$ 群表示按 D_3 约化

表示 $\{\Gamma^{(l)}\}$ 中与 D_3 相对应类的特征标 $\chi^{(l)}(g_a)$				表示 $\{\Gamma^{(l)}\}$ 约化的结果	
l	$\{E\}$	$\{C_3(2)\}$	$\{C_2(3)\}$	$SO(3)$	D_3
0	1	1	1	Γ_1	a_1
1	3	0	-1	$\Gamma_2\oplus\Gamma_3$	$a_2\oplus E$
2	5	-1	1	$\Gamma_1\oplus 2\Gamma_3$	$a_1\oplus 2e$
3	7	1	-1	$\Gamma_1\oplus 2\Gamma_2\oplus 2\Gamma_3$	$a_1\oplus 2a_1\oplus 2e$
4	9	0	1	$2\Gamma_1\oplus\Gamma_2\oplus 3\Gamma_3$	$2a_1\oplus a_1\oplus 3e$
5	11	-1	-1	$\Gamma_1\oplus 2\Gamma_2\oplus 4\Gamma_3$	$a_1\oplus 2a_2\oplus 4e$
6	13	1	1	$3\Gamma_1\oplus 2\Gamma_2\oplus 4\Gamma_3$	$3a_1\oplus 2a_2\oplus 4e$

注意，其中应用到约化公式 $m_i = \frac{1}{g}\sum_{a=1}^{c}\chi^{(l)}(g_a)\chi^{(i)}(g_a)$.]

5. 设 $\hat{H}_0 = -\frac{\hbar^2}{lm}\nabla^2 - eV(r)$，其中 $V(r)$ 是球面对称势. 如果有微扰势 $\hat{H}' = -eV'$，其中 V' 具有 D_3 对称性. 求 $\hat{H}_1$ 对 H_0 的本征态 $e = 1, S$ 的能级简并度的影响.

[提示：利用上题结果，$l = 1, \Gamma^{(1)} = \Gamma_2 \oplus \Gamma_3; l = 5, \Gamma^{(5)} = \Gamma_1 \oplus 2\Gamma_2 \oplus 4\Gamma_3$.]

6. 请将 $SO(3)$ 的不可约表示 $\Gamma^{(l)}$ 按 O 群和 O_h 群约化.

[提示：先计算 O、O_h 的特征标.]

第 6 章　Galois 群及其应用

本章介绍 19 世纪以来代数学的主要研究内容，即“近世代数”(或“抽象代数”) 的最初思想源泉 ——Galois 理论. 它既是应用多学科知识解决重大数学难题的范例，也是代数学发展史上的一个里程碑和转折点. 19 世纪初，挪威数学家 Abel 证明了五次以上的方程没有一般求解公式. 法国数学家 Galois 给出了一个给定方程有求解公式的判别准则，提出了“群”及“可解群”等新的概念. 他把方程有无公式解的问题转化为相应的群是否为可解群的问题. 他解决这一重大数学问题的思想及方法，后人称为 Galois 理论. 德国数学家 Dedekind 等人系统阐述和整理了 Galois 的理论，开始注重抽象的代数结构的研究. 从此之后，这些研究逐步形成代数学研究的主流.

本章讨论经典的Galois 理论，因而讨论的域扩张均指有限扩张. 内容包括Galois 理论的基本定理，方程可用根式解的判别准则以及Galois 理论的初步应用，旨在使学生欣赏并了解 Galois 理论的优美数学思想，了解某些世界性的数学难题是如何利用 Galois 理论得到解决的，同时也对有限群论和域论这两个代数分支的联系有进一步的认识.

§6.1　代数方程解法概述

1. 关于什么是代数学的历史观点

关于什么是代数学以及代数学的基本问题是什么这两个问题的观念，在代数学的发展史上有两次改变：一次是在 19 世纪的前半期，另一次则发生在 20 世纪初，从而把代数学的发展史相应地分为三个时期，代数学的历史不同于解析几何与数学分析的历史，后者由它们的创始人 —— 笛卡尔、牛顿、莱布尼茨等奠基后，虽然有进一步的发展，甚至用大量的新内容来补充它们，但是它们的本来面貌在原则上却没有大的改变. 而代数学在其发展的三个历史时期内，人们曾把三个很不相同的东西理解为代数学.

法国数学家韦达与笛卡尔引进了字母表示法. 从这个时候开始，人们把代数看成是关于字母计算、关于代数式的变换以及代数方程等的科学. 在那时，整个数学，无论是几何学还是数学分析都被叫做代数学，这就是关于什么是代数学的第一个观点. 欧拉的著

作《代数学引论》特别明显地体现了这一点.

在18世纪末及19世纪初,代数方程的解法问题被认为是代数学的中心回题.16世纪意大利数学家求出了解三次及四次方程的一般法则,但在长达近300年的时间里人们没能找到五次方程的解法.在这段时间里,围绕着这个问题数学家们进行了艰苦的努力,建立了大规模的复杂理论.19世纪中叶谢尔把代数学看成是解代数方程的理论,这就是关于什么是代数学的第二个观点.

19世纪后半期,由代数方程联立理论而产生的群论迅速发展起来,由于物理学等学科及数学本身的需要,越来越多地要研究一些元素(这些元素已不是单纯的数),随之很自然地要研究这些元素的运算,但这些运算却具有不同于普通数的运算规律.例如向量、矩阵、张量、旋量、超复数等,这些量都是用字母表示的,不同形式的量的运算规律也不同.这些量的某个集合对于给出的运算以及这些运算满足某些规律,组成了某一个代数系统.

代数学的中心问题就是研究各种代数系统,如群、环、域、代数、格等.这就是什么是代数学的第三个观点:研究各种代数系统的数学分支,即公理化的或抽象的代数学.

2. 代数方程解法的历史概述

如上所述,代数方程的解法曾在一个时期(18世纪末及19世纪初)被认为是代数学的中心问题,下面就这个问题再作专门的叙述.

我们知道,形如 $x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$ 的方程叫做一元 n 次方程(当最高次项系数不等于1时可以用它除方程的两边而化成这种形式),其中 a_1, a_2, $\cdots$, a_n 是某数域上给定的数,叫做方程的系数.

对于一元一次及二次方程,在阿里·花剌子模的著作中已记有一般解法.其解法公式相当简单,初中代数教材中都有关于它们的叙述.

关于高于二次的方程的解法,1541年,意大利数学家塔里塔利亚得到了三次方程的一般解法.一元三次方程的解法如下:

设一元三次方程 $y^3 + ay^2 + by + c = 0$.

令 $y = x - a/3$,得 $x^3 + px + q = 0$,这样,任何三次方程都可以化成不含平方项的三次方程($x^3 + px + q = 0$).设 $x = u + v$,所以 $x^3 = (u + v)^3 = u^3 + v^3 + 3uv(u + v)$,即 $x^3 - 3uvx - (u^3 + v^3) = 0$,比较系数得,$u^3 + v^3 = -q$,$3uv = -p$,即 $u^3 + v^3 = -q$,$u^3v^3 = -p^3/27$,由此可知,u^3、v^3 是二次方程 $z^2 + qz - p^3/27 = 0$ 的根,所以

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

每一立方根有三个不同的值,原可得出九种可能,但因 $uv = -p/3$,所以仅有下面

三种可能：

$$x_1=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

$$x_2=\left[\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\right]\cdot\omega,$$

$$x_3=\left[\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}\right]\cdot\omega^2,$$

其中 $\omega=\cos\frac{2\pi}{3}+\mathrm{i}\sin\frac{2\pi}{3}=-\frac{1}{2}+\frac{\sqrt{3}}{2}\mathrm{i},\omega^2=-\frac{1}{2}-\frac{\sqrt{3}}{2}\mathrm{i}.$

当解为实数时，可以分下面四种情况来讨论：

①$q^2/4+p^3/27<0$；　②$q^2/4+p^3/27>0$ 且 $p<0$；

③$q^2/4+p^3/27>0$ 且 $p>0$；　④$q^2/4+p^3/27=0$. 以下从略.

由于当时还没有虚数的概念，所以塔里塔利亚的公式仅限于

$$x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

三次方程解决之后，自然又提出了四次方程解法的问题，下面我们介绍四次方程的解法.

设四次方程

$$y^4+a_1y^3+a_2y^2+a_3y+a_4=0.$$

令 $y=x-a_1/4$，得 $x^4+px^2+qx+r=0$，

其中 $p=-3/8a_1^2+a_2,q=1/8a_1^3-1/2a_1a_2+a_3,r=-3/256a_1^4+1/16a_1^2a_2-1/4a_1a_3+a_4$.

因为 $x^4+px^2+qx+r=(x^2+p/2+\alpha)^2+qx+r-p^2/4-\alpha^2-2\alpha x^2-p\alpha$，所以方程可化成

$$(x^2+p/2+\alpha)^2-[2\alpha x^2-qx+(\alpha^2+p\alpha-r+p^2/4)]=0 \qquad (*)$$

方程 $2\alpha x^2-qx+(\alpha^2+p\alpha-r+p^2/4)=0$ 的判别式为：

$$\Delta=q^2-4\times2\alpha(\alpha^2+p\alpha-r+p^2/4)],$$

令 $\Delta=0$，即 $q^2-4\times2\alpha(\alpha^2+p\alpha-r+p^2/4)]=0$，

此为关于 α 的三次方程，设 α_0 为它的一个根，则对于 α_0 方程(＊)左边为完全平方式，即

$$2\alpha x^2-qx+(\alpha^2+p\alpha-r+p^2/4)=2\alpha_0(x-q/4\alpha_0)^2,$$

于是上面方程可以化成 $(x^2+p/2+\alpha)^2-2\alpha_0(x-q/4\alpha_0)^2=0$，

此方程可分解成两个二次方程：

$$x^2+\sqrt{2\alpha_0}+\left[\frac{p}{2}+\alpha_0-\frac{q}{\sqrt{2\alpha_0}}\right]=0,x^2-\sqrt{2\alpha_0}+\left[\frac{p}{2}+\alpha_0+\frac{q}{\sqrt{2\alpha_0}}\right]=0,$$

解这两个方程，便可求出方程的解，从而得到四次方程的解.

上面的解法是由意大利数学家费拉里首先发现的，故称之为“费拉里解法”.

法国数学家拉格朗日在 1770—1771 年所发表的论文《关于代数方程解法的思考》中讨论了二次、三次及四次方程的解法. 拉格朗日的推导与先前的意大利学者不同，后者对每种情况都是针对其方程的特点而找到一些变换从而得出解法，得到解法的方法是富有机智的但看起来又好像是非常偶然的，而拉格朗日则是从一个统一的原则出发借助对称多项式的理论及置换的理论得到了二次、三次、四次方程的解法. 下面以四次方程的解法为例加以说明.

在拉格朗日的解法中，他引进了式子

$$x_1+\omega x_2+\omega^2x_3+\cdots+\omega^{n-1}x_n$$

其中 $x_1,x_2,\cdots x_n$ 是 n 次方程 $x^n+a_1x^{n-1}+a_2x^2+\cdots+a_{n-1}x+a_n=0$ 的根，ω 是 1 的任一 n 次根，我们把上面的式子称为拉格朗日预解式，四次方程 $x^4+a_1x^3+a_2x^2+a_3x+a_4=0$ 的拉格朗日预解式为 $x_1+\omega x_2+\omega^2x_3+\omega^3x_4$.

显然 -1 是 1 的四次方根，取 $\omega=-1$，则此预解式变为 $x_1-x_2+x_3-x_4$，

作出 x_1、x_2、x_3、x_4 的一切排列(共 24 种)，得到六个不同的式子：

$$x_1-x_2+x_3-x_4;x_1+x_2-x_3-x_4;x_1-x_2-x_3+x_4;$$
$$-x_1+x_2-x_3+x_4;\ -x_1-x_2+x_3+x_4;\ -x_1+x_2+x_3-x_4.$$

以上述六个式子为根的六次方程的系数是对 x_1、x_2、x_3、x_4 的所有 24 种排列不变的，因为这 24 个排列中的任何一个只能把这些式子重新排列一下，而这个六次方程的系数与它的根的顺序无关，于是这些系数 a_1、a_2、a_3、a_4 确定下来了. 此外，由于上面的六个式子成对具有相反的符号，所以这个六次方程仅有偶次项，直接计算可知这个六次方程是：

$$y^6-(3a_1^2-8a_2)y^4+3(a_1^4-16a_1^2a_2-16a_2^2+16a_1a_3-64a_4)y^2$$
$$-(a_1^2-4a_1+18a_3)^2=0,$$

令 $y^2=x$，则得到 x 的三次方程. 设它的根是 α、β、γ，则

$$x_1-x_2+x_3-x_4=\sqrt{\alpha},x_1+x_2-x_3-x_4=\sqrt{\beta},x_1-x_2-x_3+x_4=\sqrt{\gamma},x_1+x_2+x_3+x_4=-a_1.$$

解这四个关于 x_1、x_2、x_3、x_4 的方程组成的方程组，即可求出原方程的四个根.

从上面的过程可以看出，解四次方程归结为解三次方程，类似地可以讨论二次、三

次方程的解法. 从中可以看出,二次、三次、四次方程的解法有一个共同的特点,即把这些方程通过一个合适的变换(如四次方程解法中的拉格朗日预解式)而化成次数较低的方程来解.

拉格朗日正确地预见到根的置换理论是解代数方程的关键.

1824 年,挪威数学家阿贝尔证明了这样一个事实:如果方程的次数不小于 5,那么任何由方程系数组成的根式都不可能是这个方程的根. 这就是说五次及五次以上的方程的根号解法是不存在的.

阿贝尔虽然证明了一般性五次及五次以上方程不能用根号解出,但并不是说任何五次及五次以上的方程都不能用根号解 . 例如二项方程 $z^n = A$ 就永远能用根号解,因此,阿贝尔的证明并不是问题的全部,代数方程理论的最美妙之处仍然留在后面,即具有什么条件的特殊的五次及五次以上的方程是可以用根号解出的呢?所以,在阿贝尔的工作之后,关于用根号解代数方程的问题以新的形式提了出来:寻求代数方程能用根号解的充分必要条件. 这个问题由法国数学家伽罗华所解决,他引入置换群的概念彻底解决了代数方程用根号解的条件问题,从而开辟了代数学的一个崭新的领域 —— 群论.

围绕着用根号解代数方程的问题,人类付出了长达三个世纪之久的艰苦劳动,最终由两位年轻的数学家给予了彻底而圆满的解答. 他们的解答所带来的不仅是问题本身的解决,而是开创了代数学发展史上的新纪元. 从此,关于抽象群的理论迅速发展起来. 而代数学则被认为是研究代数系统的数学分支,这就是什么是代数学的第三个观点.

前面曾经提到,法国数学家拉格朗日在 1770—1771 年所发表的论文《关于代数方程解法的思考》中曾注意到根的置换,并正确地预见到根的排列理论是整个问题的关键. 1815 年法国数学家柯西系统地研究了置换群的理论. 更一般的群的概念是伽罗华在 1832 年引进的. 直到 1854 年,英国数学家凯莱才给出一般抽象群的定义,他不仅彻底解决了用根号解代数方程的问题,而且开始了代数学发展的新时期 —— 近世代数时期.

§6.2　Galois 基本定理

设 F 是域 E 的子域,令 $\mathrm{Aut}(E)$ 是正的所有自同构作成的集,则 $\mathrm{Aut}(E)$ 关于映射的合成是群. 令

$$G(E/F) = \{\sigma \in \mathrm{Aut}(E), \sigma(a) = a, \forall\, a \in F\},$$

则可验证 $G(E/F)$ 是 $\mathrm{Aut}(E)$ 的子群. 设 $G \leqslant G(E/F)$,令

$$E^G = \{a \in E \mid \sigma(a) = a, \forall\, \sigma \in G\},$$

则 E^G 是域. E^G 称为群 G 的固定域. 若 $F \subset K \subset E$ 且是域,则称 K 是中间域,若把 E 看

作 F 上向量空间,E 在 F 上的维数称为 E 在 F 上的次数,记为$[E:F]$.

例如,设 F 是有理数域,$E=Q(\sqrt{2})$,则 $G(E/F)=\{1,f\}$,

其中 $f:a+b\sqrt{2}\to a-b\sqrt{2},a,b\in F$. 从而 $E^{G(E/F)}=F$.

下面的命题揭示了多项式的根与系数之间的关系,是韦达定理的推广.

命题 6.2.1 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$ 是域 F 上的 n 次多项式,E 是 $f(x)$ 的分裂域,则 $f(x)=(x-z_1)(x-z_2)\cdots(x-z_n)$,其中 $z_i\in E$,有下列结果:

$$a_{n-1}=-\sum_i z_i,a_{n-2}=\sum_{i<j}z_iz_j,a_{n-3}=-\sum_{i<j<k}z_iz_jz_k\cdots a_0=(-1)^nz_1z_2\cdots z_n.$$

称为关于 $z_1,z_2\cdots z_n$ 的初等多项式.

命题 6.2.2 设 $f(x)$ 是域 F 上的可分多项式,E 是 $f(x)$ 在 F 上的分裂域,$\alpha\in E$,是 $f(x)$ 的一个根,则对于 $\forall\ \sigma\in G(E/F)$,$\sigma(\alpha)$ 也是 $f(x)$ 的一个根. 进而,σ 是 $f(x)$ 的所有根的集合上的一个置换.

证明 设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$

则 $\qquad f(\sigma)=\sigma^n+a_{n-1}\sigma^{n-1}+\cdots+a_1\sigma+a_0I=0$

用 σ 对方程两边进行变换,注意到 σ 保持 F 中元不动,我们有

$$\begin{aligned}f(\sigma(\alpha))&=\sigma(\alpha)^n+a_{n-1}\sigma(\alpha)^{n-1}+\cdots+a_1\sigma(\alpha)+a_0\\&=\sigma(\alpha)^n+\sigma(a_{n-1})\sigma(\alpha)^{n-1}+\cdots+\sigma(a_1)\sigma(\alpha)+\sigma(a_0)=0.\end{aligned}$$

所以 $\sigma(\alpha)$ 是 $f(x)$ 的一个根,设 S 是 $f(x)$ 的 n 个根组成的集合,因 σ 是单射,所以 σ 在 S 上的限制 $\sigma|_S:S\to S$ 是单射,即对于 $\eta\in S,\sigma|_S(\eta)=\sigma(\eta)$. 这样 $\sigma|_S$ 是 S 的一个置换.

由命题 6.2.2,我们经常说 σ 置换 $f(x)$ 的根,也说 $G(E/F)$ 置换 $f(x)$ 的根. 由于 $f(x)$ 的系数都是关于它们根的初等对称多项式,因而 $G(E/F)$ 置换 $f(t)$ 的根意味着 $G(E/F)$ 中任意元保持 $f(x)$ 的每项系数不动. 这一简单事实在 Galois 理论中经常用到. 事实上,利用多项式根的所有置换作成的集合的性质来讨论多项式方程是否有根式解是 Galois 理论的思想源泉之一.

命题 6.2.3 设 $S=\{\varphi_1,\varphi_2,\cdots,\varphi_n\}\subseteq\mathrm{Aut}(E)$ 是一个 n 元子集,E^S 是 S 的固定域,则$[E:E^S]\geqslant n$.

证明 设 $|E:E^S|=m<n,\alpha_1,\alpha_2,\cdots,\alpha_m$ 是 E 在 E^S 上的一个基,考虑齐次线性方程组

$$\begin{cases}x_1\varphi_1(\alpha_1)+\cdots+x_n\varphi_n(\alpha_1)=0,\\x_1\varphi_1(\alpha_2)+\cdots+x_n\varphi_n(\alpha_2)=0,\\\qquad\cdots\cdots\\x_1\varphi_1(\alpha_m)+\cdots+x_n\varphi_n(\alpha_m)=0.\end{cases}\tag{2.1}$$

因为 $m < n$，故方程组在 E 中有非零解.

任取 $\alpha \in E$，则 $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_m\alpha_m$，其中 $\alpha_i \in E^S$，于是对 $\forall\ \varphi \in S$，我们有

$$\varphi(\alpha) = a_1\varphi(\alpha_1) + a_2\varphi(\alpha_2) + \cdots + a_m\varphi(\alpha_m). \tag{2.2}$$

对于 $i = 1, 2, \cdots, m$，用 a_i 乘方程组(2.1)的第 i 个方程，然后相加得

$$\begin{aligned} &a_1x_1\varphi_1(\alpha_1) + a_1x_2\varphi_2(\alpha_1) + \cdots + a_1x_n\varphi_n(\alpha_1) + a_2x_1\varphi_1(\alpha_2)\\ &\quad + a_2x_2\varphi_2(\alpha_1) + \cdots + a_2x_n\varphi_n(\alpha_2) + \cdots + a_mx_1\varphi_1(\alpha_m)\\ &\quad + a_mx_2\varphi_2(\alpha_m) + \cdots + a_mx_n\varphi_n(\alpha_m) = 0, \end{aligned} \tag{2.3}$$

将式(2.3)按列相加并利用式(2.2)我们有

$$x_1\varphi_1(\alpha) + x_2\varphi_2(\alpha) + \cdots + x_n\varphi_n(\alpha) = 0, \text{对}\ \forall\ \alpha \in E\ \text{成立}. \tag{2.4}$$

在方程组(2.1)的所有非零解中，设 $c_1, c_2, \cdots, c_n$ 是所有解当中包含零最多的一个解. 不失一般性，不妨设 $c_1, c_2, \cdots, c_j \neq 0$，$c_{j+1}, c_{j+2}, \cdots, c_n = 0$，于是我们有

$$c_1\varphi_1(\alpha) + c_2\varphi_2(\alpha) + \cdots + c_j\varphi_j(\alpha) = 0, \tag{2.5}$$

因为 $c_i \neq 0$，故 $j > 1$，从而 $\varphi_1 \neq \varphi_j$. 于是存在 $\beta \in E$ 使得 $\varphi_1(\beta) \neq \varphi_j(\beta)$. 又方程(2.4)对 E 中所有元均成立，于是我们有

$$c_1\varphi_1(\alpha\beta) + c_2\varphi_2(\alpha\beta) + \cdots + c_j\varphi_j(\alpha\beta) = 0, \tag{2.6}$$

用 $\varphi_j(\beta)$ 乘方程(2.5)与上式相减得：

$$c_1(\varphi_1(\beta) - \varphi_j(\beta))\varphi_1(\alpha) + \cdots + c_{j-1}(\varphi_{j-1}(\beta)\varphi_j(\beta))\varphi_{j-1}(\alpha) = 0, \tag{2.7}$$

可以验证 $c_1(\varphi_1(\beta) - \varphi_j(\beta)), \cdots, c_{j-1}(\varphi_{j-1}(\beta) - \varphi_j(\beta))$ 是方程组(2.1)的一个解. 方程(2.7)关于 $\varphi_i(\alpha), i = 1, 2, \cdots, j-1$ 的系数不全为零，而在(2.7)中最多有 $j-1$ 项不为零，这与(2.5)的选择矛盾，因而必有 $[E:E^S] = m \geqslant n$.

定理 6.2.4　设 E 是 F 的扩域，下列条件等价：

1) $F = E^{G(E/F)}$；

2) $[E:F] = |E^{G(E/F)}|$；

3) E 是 F 的有限可分正规扩域；

4) E 是 F 上某个可分多项式的分裂域.

证明　1) $\Leftrightarrow$ 2). 设 $G(E/F) = \{\varphi_1, \varphi_2, \cdots, \varphi_n\}$，由条件及命题 6.2.3 知，$[E:F] \geqslant n$. 设 $[E:F] \geqslant n+1$，至少存在 E 中 $n+1$ 个元 $\alpha_1, \alpha_2, \cdots, \alpha_{n+1}$ 在 F 上无关，考虑齐次线性方程组：

$$\begin{cases} x_1\phi_1(\alpha_1) + \cdots + x_{n+1}\phi_1(\alpha_{n+1}) = 0,\\ x_1\phi_2(\alpha_1) + \cdots + x_{n+1}\phi_2(\alpha_{n+1}) = 0,\\ \qquad\cdots\cdots\\ x_1\phi_n(\alpha_1) + \cdots + x_{n+1}\phi_n(\alpha_{n+1}) = 0 \end{cases} \tag{2.8}$$

中方程的个数小于未知数个数，故(2.8)在 E 中有非零解，因为 $\alpha_1,\alpha_2,\cdots,\alpha_{n+1}$ 线性无关，所以这些解不全在 F 中，再设 $a_1,a_2,\cdots,a_{n+1}$ 是所有解中包含零最多的一个，不妨设 $a_i\neq 0(i<r)$，$a_r=1$，$a_j=0(j>r)$，则我们有

$$\begin{cases}a_1\phi_1(\alpha_1)+\cdots+\phi_1(\alpha_r)=0,\\ a_1\phi_2(\alpha_1)+\cdots+\phi_2(\alpha_r)=0,\\ \quad\cdots\cdots\\ a_1\phi_n(\alpha_1)+\cdots+\phi_n(\alpha_r)=0.\end{cases}\tag{2.9}$$

又 $a_1,a_2,\cdots,a_{r-1}$ 不全在 F 中，于是至少存在一个 $i(1\leqslant i\leqslant r-1)$ 和一个 $j(1\leqslant j\leqslant n)$ 使得 $\varphi_j(a_j)\neq a_j$，不妨设 $a_1\notin F$ 且 $\varphi_j(a_1)\neq a_1$，用 φ 作用(2.9)式的两边，有 $\varphi_j(a_1)\varphi_j\phi_i(\alpha_1)+\cdots+\varphi_j(a_r)\varphi_j\phi_i(\alpha_r)=0\quad(i=1,2,\cdots,n)$

即
$$\begin{cases}\varphi_j(a_1)\varphi_j\phi_1(\alpha_1)+\cdots+\varphi_j(a_r)\varphi_j\phi_1(\alpha_r)=0,\\ \varphi_j(a_1)\varphi_j\phi_2(\alpha_1)+\cdots+\varphi_j(a_r)\varphi_j\phi_2(\alpha_r)=0,\\ \quad\cdots\cdots\\ \varphi_j(a_1)\varphi_j\phi_n(\alpha_1)+\cdots+\varphi_j(a_r)\varphi_j\phi_n(\alpha_r)=0.\end{cases}\tag{2.10}$$

式(2.9)与式(2.10)对应方程相减得

$$(a_1-\varphi_j(a_1))\varphi_j\phi_i(\alpha_1)+\cdots+(a_{r-1}-\varphi_j(a_{r-1}))\varphi_j\phi_i(\alpha_{r-1})=0(i=1,2,\cdots,n)$$

这里 $i=1,2,\cdots,n$，我们知道 $a_1-\varphi_j(a_1)\neq 0$，这就有方程组(2.10)，从而方程组(2.8)有非零解 $b_1=a_1-\varphi_j(a_1),b_2,\cdots,b_n$ 满足 $b_r=b_{r+1}=\cdots=b_n=0$，这与假设矛盾. 于是我们有 $[E:F]=|E^{G(E/F)}|$；

反之由定义可知，$F\subseteq E^{G(E/F)}$，于是 $[E:E^{G(E/F)}][E^{G(E/F)}:F]=[E:F]=|E^{G(E/F)}|$，由此得 $[E^{G(E/F)}:F]=1$，也即 $E^{G(E/F)}=F$.

1) $\Leftrightarrow$ 3). 设 $F=E^{G(E/F)}$，$p(x)$ 是 F 上不可约多项式，$\alpha\in E$ 是 $p(x)$ 的一个根. 设 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 是 α 在 $G(E/F)$ 作用下 E 中所有互不相同的根，不妨设 $\alpha=\alpha_1$，下面证 $p(x)$ 在 $E[x]$ 中能分解成一次因式之积，从而 E 是 F 的正规扩域.

因为 $p(\alpha)=0$，故在 $E[x]$ 中，$p(x)=(x-\alpha)q(x)$. 设 $\sigma\in G(E/F)$，则 σ 以一种明显的方法可扩展为 $E[x]$ 的一个自同构，于是对某个整数 i，我们有

$$p(x)=\sigma(p(x))=(x-\sigma(\alpha))\sigma(q(x))=(x-\alpha_i)\sigma(q(x)).$$

这就是说，每个 $x-\alpha_i$ 是 $p(x)$ 在 $E[x]$ 中的一个因子，于是我们有

$$p(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)h(x).$$

设 $s(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$，

则 $s(x)$ 的系数是 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 的初等对称多项式，故它在 $\sigma\in G(E/F)$ 作用下保持不动，故 $\sigma(s(x))=s(x)$.

又由假设 $F=E^{G(E/F)}$ 知 $s(x)\in F[x]$.

这样从 $p(x)=\sigma(p(x))=\sigma(s(x))\sigma(h(x))$ 可得 $\sigma(h(x))=h(x)\in F[x]$.

但 $p(x)$ 是 $F[x]$ 上的不可约多项式，故 $h(x)=c\in F$，即 $p(x)$ 在 $E[x]$ 中分解成一次因式之积，由以上证明知 $p(x)$ 在 E 内无重根，即 $p(x)$ 是可分多项式，由 $p(x)$ 的任意性知，$F[x]$ 中任意不可约多项式都是可分多项式，即 E 是 F 的可分扩域.

反之，设 E 是域 F 的有限可分正规扩域，要证 $F=E^{G(E/F)}$，只需证 $E^{G(E/F)}\subseteq F$. 设 $\alpha\in E$ 但 $\alpha\notin F$，令 $p(x)$ 是 α 在 F 上的不可约多项式，由假设知 $p(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$，其中 $\alpha_i\in E,\alpha_1,\alpha_2,\cdots,\alpha_n$ 两两互不相同. 令 $\alpha_1=\alpha$，因为 $\alpha\notin F$，故 $n=\deg f(x)>1$，因而 $\alpha_2\neq\alpha$.

设 F 是域，$p(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ 是 $F[x]$ 的不可约多项式，则存在 F 的单代数扩域 $F(\alpha)$，其中 α 在 F 上的极小多项式是 $p(x)$. 若 β 在 F 上的极小多项式也是 $p(x)$，则存在同构映射 φ 使得 $F(\alpha)\cong F(\beta)$ 且 $\varphi(\alpha)=\beta$. 知存在 $\sigma\in G(E/F)$ 使得 $\sigma(\alpha)=\alpha_2\neq\alpha$，故 $\alpha\notin E^{G(E/F)}$，这说明 $E^{G(E/F)}\subseteq F$，这正是要证的结论.

1) $\Leftrightarrow$ 4). 设 $F=E^{G(E/F)}$，$\xi_1,\xi_2,\cdots,\xi_n$ 是 E 在 F 上的一个基，则 E 是 F 的代数扩域. 不妨设 ξ_i 在 F 上的不可约多项式是 $p_i(x)$，因为 1) 可得 3)，故 $p_i(x)(i=1,2,\cdots,n)$ 的所有的根均在 E 中，这说明 E 是多项式 $p(x)=\mathrm{lcm}(p_1(x),\cdots,p_n(x))$ 的分裂域. 显然 $p(x)$ 无重根，也即 $p(x)$ 是 $F[x]$ 的可分多项式.

反之，设 $p(x)\in F[x]$ 是可分多项式，E 是 $p(x)$ 的分裂域，下证 $F=E^{G(E/F)}$，对 E 在 F 上的次数用归纳法. 若 $[E:F]=1$，成立.

设 $[E:F]=n$，E 是 $p(x)=p_1(x)p_2(x)\cdots p_t(x)\in F[x]$ 的分裂域，其中 $p_1(x)$ 是 $k(>1)$ 次不可约多项式，其根为 $\alpha_1,\alpha_2,\cdots,\alpha_k$，于是 $[F(\alpha_1):F]=k>1$. 令 $K=F(\alpha_1)$，则 $[E:K]=[E:F]/[K:F]=n/k\leqslant n-1$，且 E 也是 $p(x)$ 在 K 上的分裂域，由假设 $K=E^{G(E/F)}$，知对于 $\forall\,\alpha\in E,\varphi\in G(E/K)$，只要 $\alpha=\varphi(\alpha)$，则必有 $\alpha\in K$. 从而 $\alpha=a_0+a_1\alpha_1+\cdots+a_{k-1}\alpha_1^{k-1}$，其中 $a_i\in F$.

现在我们要证明对于 $\forall\,a\in E,\sigma\in G(E/F)$，只要 $a=\sigma(a)$，则必有 $a\in F$，现在设 $a\in E,\sigma\in G(E/F)$，且 $a=\sigma(a)$，因为每个保持 K 不变的自同构也使 F 不变，故 a 被每一个 $\varphi\in G(E/K)$ 固定，因为 $p(x)$ 是可分多项式，从而 $p_1(x)$ 也是可分多项式. $F(\alpha_1)\cong F(\alpha_i)(i=1,2,\cdots,k)$ 且对每个 i 存在 $\sigma_i\in G(E/F)$，使得 $\sigma_i(\alpha_1)=\alpha_i$，因而我们有

$$a=\sigma_i(a)=\sigma_i(a_0+a_1\alpha_1+\cdots+a_{k-1}\alpha_1^{k-1})=a_0+a_1\alpha_i+\cdots+a_{k-1}\alpha_i^{k-1}$$

令

$$r(x)=(a_0-a)+a_1x+\cdots+a_{k-1}x^{k-1},$$

由上式这是 K 上具有根 $\alpha_1,\alpha_2,\cdots,\alpha_k$ 的 $k-1$ 次多项式，然而 $k-1$ 次多项式在 K 中至多有 $k-1$ 个根，从而 $r(x)=0$. 由此得 $a_0-a=0$，也即 $a=a_0\in F$，这正是我们要证的结论.

推论 6.2.5　设 E 是域 F 的扩域，$G \leqslant \mathrm{Aut}(E)$ 是 n 阶子群，则：

1) 若 $\varphi \in \mathrm{Aut}(E)$ 固定 E^G，则 $\varphi \in G$；

2) 若 G_1 和 G_2 是 $\mathrm{Aut}(E)$ 的两个不同的有限子群，则 $E^{G_1} \neq E^{G_2}$.

证明　1) 若 $\varphi \notin G$，则 E^G 在 E 的 $n+1$ 个自同构作用下保持不动，于是 $[E:E^G] \geqslant n+1$. 另一方面，$|E:E^G| = n$ 矛盾.

2) 若 $E^{G_1} = E^{G_2}$，则 E^{G_1} 也被 G_2 固定，由 1) 可知 $C_2 \leqslant G_1$. 类似地也有 $G_1 \leqslant G_2$，从而 $G_1 = C_2$ 矛盾.

设 E 是域 F 的扩域，E 称为 F 的 Galois 扩域（或 Galois 扩张），若 E 满足定理 6.2.4 的 1)、2)、3) 及 4) 中的任意一条，记为 E/F（或 $F \lhd E$）. 相应地，$G(E/F)$ 称为 Galois 扩张 E/F 的 Galois 群. 若 $f(x) \in F[x]$，E 是 $f(x)$ 在 F 上的分裂域，则 $G(E/F)$ 也称为 $f(x)$ 在 F 上的 Galois 群，或方程 $f(x)=0$ 在 F 上的 Galois 群. 不失一般性，一个扩域的 Galois 群与一个多项式的 Galois 群没有实质性的区别. 另外，若 E/F 是 Galois 扩张，K 是 F 的中间域，则 E/K 也是 Galois 扩张，这一简单事实我们以后要用到.

例 6.2.1　设 $E = Q(\sqrt{2}, \sqrt{3})$，计算 $G(E/Q)$.

解　E 是 $f(x) = (x^2-2)(x^2-3)$ 在 Q 上的分裂域且 $[E:Q]=4$，因而 E/Q 是 Galois 扩张. E 的每个元可唯一表示为 $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$，其中 $a,b,c,d \in Q$. 因为 $G(E/Q)$ 的每个元置换 $f(x)$ 的根，于是 E 的每个自同构 σ 完全由它在 $\sqrt{2}$，$\sqrt{3}$ 上的作用确定，因而仅有的可能性只能是

$$\sigma: \sqrt{2} \longmapsto -\sqrt{2}, \sqrt{3} \longmapsto \sqrt{3}; \tau: \sqrt{2} \longmapsto \sqrt{2}, \sqrt{3} \longmapsto -\sqrt{3}.$$

通过计算易得，$\sigma^2 = \tau^2 = I$，因为 $G(E/Q) = 4$，故 $G(E/Q) = \{I, \sigma, \tau, \sigma\tau\}$，由此可见 $G(E/Q)$ 是 Klein 四元群.

例 6.2.2　设 $E = Q(\sqrt[3]{2})$，计算 $G(E/Q)$.

解　$\sqrt[3]{2}$ 在 Q 上的不可约多项式为 x^3-2. 它的另两个根分别为 $\sqrt[3]{2}\omega$，$\sqrt[3]{2}\omega^2$，其中 ω 为三次本原单位根. 由于 $G(E/Q)$ 中元 σ 置换 x^3-2 的根，而 $\omega \notin E$，故 $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$，从而 $\sigma = 1$，即 $G(E/Q) = 1$. 但 $[E:Q] = 3$，因而 E/Q 不是 Galois 扩张.

定义 6.2.1　设 E 是 F 的有限扩域，K_1, K_2 是中间域，域 K_2 称为与 K_1 共轭，若存在 $\sigma \in \mathrm{Aut}(E)$ 使得 σ 在 F 上是恒等映射且 $\sigma(K_1) = K_2$. 这样的 σ 称为 F 自同构. 若对 $\forall\, \sigma \in G(E/F)$ 都有 $\sigma(K) = K$，则 K 称为 F 的自共轭扩张. 对于 $\alpha_1, \alpha_2 \in E$，称 α_1 为与 α_2 共轭，若存在 $\sigma \in \mathrm{Aut}(E)$ 使得 σ 在 F 上是恒等映射且 $\sigma(\alpha_1) = \alpha_2$.

定理 6.2.6　设 E 是 F 的 Galois 扩张，$F < K_1, K_2 < E$，则 K_1 与 K_2 共轭，$G(E/K_1)$ 与 $G(E/K_2)$ 是 $G(E/F)$ 的共轭子群.

证明　设 K_1 与 K_2 共轭，σ 是相应的 F 自同构，于是对 $\forall\, \alpha_2 \in K_2$，存在 $\alpha_1 \in K_1$ 使得 $\sigma(\alpha_1) = \alpha_2$，设 $\varphi \in G(E/K_1)$，则 $\varphi(\alpha_1) = \alpha_2$. 于是

$$\alpha_2 = \sigma(\alpha_1) = \sigma(\varphi(\alpha_1)) = \sigma(\varphi\sigma^{-1}(\alpha_2)) = \sigma\varphi\sigma^{-1}(\alpha_2),$$

这说明 $\sigma\varphi\sigma^{-1} \in G(E/K_2)$. 类似地，对每个 $\psi \in G(E/K_2)$，可证 $\sigma\psi\sigma^{-1} \in G(E/K_1)$，由此可得 $G(E/K_1)$ 与 $G(E/K_2)$ 共轭.

反之设 $G(E/K_1)$ 与 $G(E/K_2)$ 是 $G(E/F)$ 的共轭子群，于是存在 $\sigma \in G(E/F)$，使得 $\sigma G(E/K_1)\sigma^{-1} = G(E/K_2)$.

下证 $\sigma(K_1) = K_2$. 设 $\alpha_2 \in K_2$，对每个 $\varphi \in G(E/K_1)$，我们有 $\sigma\varphi\sigma^{-1} \in G(E/K_2)$，因而 $\sigma\varphi\sigma^{-1}(\alpha_2) = \alpha_2$，或 $\varphi(\sigma^{-1}(\alpha_2)) = \sigma^{-1}(\alpha_2)$.

这说明 $\sigma^{-1}(\alpha_2)$ 被 φ 固定. 由假设 E 是 F 的Galois 扩域，易知 E 也是 K_1 的 Galois 扩域. 又 K_1 是 $G(E/K_1)$ 的固定域，因而 $\sigma^{-1}(\alpha_2) \in K_1$. 这说明 $\sigma^{-1}(K_2) \subseteq K_1$，或 $K_2 \subseteq \sigma(K_1)$.

另一方面，$\sigma\varphi\sigma^{-1}(\sigma(\alpha_1)) = \sigma\varphi(\sigma^{-1}\sigma(\alpha_1)) = \sigma\varphi(\alpha_1) = \sigma(\alpha_1)$. 因为 $\sigma G(E/K_1) = G(E/K_2)$，$K_2$ 是 $G(E/K_2)$ 的固定域. 这说明 $\sigma(\alpha_1) \in K_2$，也即 $\sigma(K_1) \subseteq K_2$，从而 $\sigma(K_1) = K_2$.

定理 6.2.7　设 E 是 F 的 Galois 扩域，K 是中间域，则 $F \lhd K$ 当且仅当 K 是 F 的自共轭扩张.

证明　由定理 4.2.4 知，$F \lhd K \Leftrightarrow K$ 是 $F[x]$ 的某个可分多项式的分裂域，因而我们只需证明 K 是 $F[x]$ 的某个可分多项式的分裂域当且仅当 K 是 F 的自共轭扩张.

设 K 是 $F[x]$ 的可分多项式 $p(x)$ 的分裂域，令 $\sigma \in G(E/F)$，则 $\sigma(p(x)) = p(x)$. 设 α 是 $p(x)$ 在 K 里的一个根，则 $\sigma(\alpha)$ 也是 $p(x)$ 的根，且 σ 置换 $p(x)$ 的所有根. 由分裂域的定义可知，σ 把 K 变到 K，即 $\sigma(K) = K$. 故 K 是自共轭扩张.

反之，设 K 是 F 的自共轭扩张，不妨设 $F < K < E$，因 E 是 F 的有限可分扩域，故 K 是 F 的有限可分扩域，K 是 F 的单扩域. 设 $K = F(\alpha)$，再令 $\alpha_1, \alpha_2, \cdots, \alpha_n$ 是 α 在 $G(E/F)$ 作用下所有两两不同的共轭元，即对 $\forall\, \alpha_i$，存在 $\sigma \in G(E/F)$ 使得 $\alpha_i = \sigma(\alpha)$，对于 $\forall\, \varphi \in G(E/F)$，由题设 $\varphi(K) = K$，故 $\alpha_i \in K(i = 1, 2, \cdots, n)$. 又 φ 置换 $\alpha_1, \alpha_2, \cdots, \alpha_n$，从而 φ 保持多项式 $p(x) = (x - \alpha_1)\cdots(x - \alpha_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ 的系数不动，因为 E 是 F 的 Galois 扩张，故 $a_i \in F$，从而 $p(x) \in F[x]$. 这说明 K 是可分多项式 $p(x)$ 的分裂域.

推论 6.2.8　设 E 是 F 的 Galois 扩域，K 是中间域，则

$$F \lhd K \Leftrightarrow G(E/K) \lhd G(E/F).$$

若 H_1, H_2 是群 G 的子群，用符号 (H_1, H_2) 表示由 H_1 和 H_2 生成的子群，若 E_1, E_2 是域 E 的子域，用符号 $\cap\,(E_1, E_2)$ 表示所有包含 E_1 与 E_2 的子域的交，它仍是 E 的子

域.

定理 6.2.9(Galois 基本定理)　设 E/F 是有限 Galois 扩张，又 E 分别是 K_1, K_2 的 Galois 扩张，由定理 6.2.4 得：$E^{G(E/K_1)} = K_1, E^{G(E/K_2)} = K_2$，所以 σ 是单射. 其对应的 Galois 群为 $G = G(E/F), K, K_1, K_2$ 是 F 与 E 的中间域，H, H_1, H_2 是 G 的子群，则：

1) 在 E 的子域 K 与 G 的子群 H 之间有一个一一对应 $\sigma: K \to G(E/K)$ 使得 $K \longmapsto H \Leftrightarrow K = E^H$. 在 G 的子群 H 与 E 的子域 K 之间也有一个一一对应 $\varphi: H \to E^H$ 使得 $H \longmapsto K \Leftrightarrow H = G(E/K)$.

进一步地，$H_2 < H_1 \Leftrightarrow E^{H_{11}} < E^{H_2}$，此时 σ, φ 称为反序对应；

2) $[E:K] = |G(E/K)|, [K:F] = [G(E/F):G(E/K)]$；

3) $F \lhd K \Leftrightarrow G(E/K) \lhd G(E/F)$，$F \lhd K$ 时，$G(K/F) \cong G(E/F)/G(E/K)$；

4) K_1 和 K_2 是共轭子域 $\Leftrightarrow G(E/K_1)$ 和 $G(E/K_2)$ 是共轭子群；

5) $E^{(H_1, H_2)} = E^{H_1} \cap E^{H_2}, E^{H_1 \cap H_2} = (E^{H_1}, E^{H_2})$,

$G(E/(K_1, K_2) = G(E/K_1) \cap G(E/K_2)$,

$G(E/(K_1 \cap K_2) = G(E/K_1), G(E/K_2)$.

证明　1) 设 $M = \{K \mid K$ 是 E 的包含 F 的子域$\}$，$V = \{H \mid H$ 是 G 的子群$\}$，令 $\sigma: M \to V$，其中 $\sigma(K) = G(E/K)$，任意 $K_1, K_2 \in M$，若 $K_1 = K_2$，由定义即得 $G(E/K_1) = G(E/K_2)$. 故 σ 是 M 到 V 的一个映射. 又若 $G(E/K_1) = G(E/K_2)$，即 $G(E/K_1) = G(E/K_2)$，则 $E^{G(E/K_1)} = E^{G(E/K_2)}$. 设 $H \in V$，令 $K = E^H$，则 $K \in M, \sigma(K) = G(E/K) = G(E/E^H)$.

又 E 是 E^H 的 Galois 扩张，故 $E^H = K = E^{G(E/K)}$，又 $H = G(E/E^H)$，故 σ 是满射，从而 σ 是 M 到 V 的一一对应. 若 $\sigma(K) = H$，由定义得 $G(E/K) = H$，从而 $E^{G(E/K)} = E^H$，又 E 是 K 的 Galois 扩张，从而 $K = E^{G(E/K)} = E^H$，结合上述满射的证法，我们有 $\sigma(K) = H \Leftrightarrow K = E^H$.

2) 因为 $E/F, E/K$ 是 Galois 扩张，由定理 6.2.4 知，

$[E:F] = |G(E/F)|, [E:K] = |G(E/K)|$；

又 $[E:K] = [E:K][K:F]$,

从而 $[K:F] = |G(E/F)/G(E/K)|$；

又 $G(E/K) \leqslant G(E/F)$，故 $[K:F] = [G(E/F):G(E/K)]$；

3) 只需证 $G(E/F) \cong G(E/F)/G(E/K)$.

因为 K 是 F 的 Galois 扩张，是对 $\forall\, \tau \in G(E/F)$，$\tau$ 限制在 K 上诱导出 K 的一个自同构，记为 $\tau|_K$. 现在我们定义 $\varphi: G(E/F) \to G(K/F)$，其中 $\varphi(\tau) = \tau|_K$.

下证 φ 是同态满射，且 $\mathrm{Ker}\varphi = G(E/K)$，从而结论得证.

首先，直接验证可知 φ 是群同态，又 $\tau \in \mathrm{Ker}\varphi \Leftrightarrow \tau|_K$ 是 K 的恒等自同构 $\Leftrightarrow \tau \in$

$G(E/K)$，即 $\mathrm{Ker}\varphi = G(E/K)$，于是由群的同态基本定理得 $G(E/F)/G(E/K) \cong \mathrm{Im}\varphi$. 因为 K 是 F 的 Galois 扩张，得 $[K:F] = |G(K/F)|$，于是由2）即得 $\mathrm{Im}\varphi = G(K/F)$.

4）由定理 6.2.6 即得；

5）设 $1 \leqslant H_1, H_2 \leqslant G$，则由定义得 $H_1, H_2 \leqslant (H_1, H_2)$，因为 τ 是反序对应，故 $\tau(H_1, H_2) \leqslant \tau(H_1), \tau(H_2)$. 由此得 $\tau(H_1, H_2) \leqslant \tau(H_1) \cap \tau(H_2)$.

又 τ 是满射，存在 $H \leqslant G$ 使 $\tau(H_1) \cap \tau(H_2) = \tau(H)$，从而 $\tau(H) \leqslant \tau(H_1), \tau(H_2)$.

因为 τ^{-1} 也是反序对应，用 τ^{-1} 作用于两边得 $H \geqslant H_1, H_2$，从而 $H \geqslant (H_1, H_2)$.

另一方面，$\tau(H_1, H_2) \leqslant \tau(H_1) \cap \tau(H_2) = \tau(H)$，用 τ^{-1} 作用两边又得 $(H_1, H_2) \geqslant H$，于是有 $H = (H_1, H_2)$，从而 $\tau(H_1, H_2) = \tau(H) = \tau(H_1) \cap \tau(H_2)$，这说明 $E^{(H_1, H_2)} = E^{H_1} \cap E^{H_2}$. 类似地可证其他等式.

例 6.2.3　设 $Q(\sqrt{2}, \sqrt{3}) = E$，确定域扩张 E/Q 的所有子域与它的 Galois 群 $G = G(E/Q)$ 的所有子群之间的关系.

已知 $G = \{I, \sigma, \tau, \sigma\tau\}$. 它有 5 个子群 $\{I\}, \{I, \sigma\}, \{I, \tau\}, \{I, \sigma\tau\}$ 和 G. 再由例 6.2.2 可知，I 的固定域为 E，$\{I, \sigma\}$ 的固定域为 $Q(\sqrt{3})$，$\{I, \tau\}$ 的固定域为 $Q(\sqrt{2})$，$\{I, \sigma\tau\}$ 的固定域为 $Q(\sqrt{6})$ 以及 G 的固定域为 Q. 容易验证 Galois 理论的基本定理的 1）～5）成立.

例如 G 的三个二阶子群是 G 的正规子群，而它们对应的固定域也都是 Q 的 Galois 扩张. 用图 6.1 可直观地解释 Galois 群的子群与其对应的固定域之间的关系.

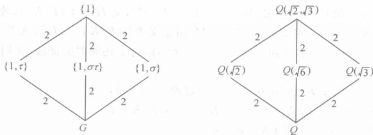


图 6.1

图 6.1 中的例子“较充分地”解释了 Galois 理论的基本定理.

例 6.2.4　设 $E = Q(\sqrt[4]{2}, \mathrm{i})$，其中 $\mathrm{i}^2 = -1$，确定域扩张 E/Q 的所有子域与它的 Galois 群 $G = G(E/Q)$ 的所有子群之间的关系.

第一步，首先考察 E 是 Q 的有限可分正规扩域；令 $f(x) = x^4 - 2$. $f(x)$ 在 Q 上不可约，它在 C 上可分解为

$f(x)=(x-\omega)(x+\omega)(x-\omega\mathrm{i})(x+\omega\mathrm{i})$,(其中 $\omega=\sqrt[4]{2}$).

于是 E 是 $f(x)$ 在 Q 上的分裂域. E 是 Q 的有限可分正规扩域. 因 $\mathrm{i}\notin Q(\omega)$,于是

$[E:Q]=[E:Q(\omega)][Q(\omega):Q]=2\times 4=8.$

第二步,确定 G 的元素. 分别记 $f(x)=x^4-2$ 的四个根为

$x_1=\sqrt[4]{2},x_2=\mathrm{i}\sqrt[4]{2},x_3=-\sqrt[4]{2},x_4=-\mathrm{i}\sqrt[4]{2}$,

直接验证或应用定理 6.5.6 我们可知

$\sigma(\mathrm{i})=\mathrm{i},\sigma(\omega)=\omega\mathrm{i},\tau(\mathrm{i})=-\mathrm{i},\tau(\omega)=\omega$

是 E 的两个 Q 自同构,它们的乘积得到 E 的 8 个 Q 自同构,这 8 个自同构是:

$I=(1),\sigma=(1234);\tau=(24);\sigma^2=(13)(24);\sigma^3=(1432)$;

$\sigma\tau=(12)(34);\sigma^2\tau=(13);\sigma^3\tau=(14)(23)$.

G 是 S_4 的 Sylow-2 子群.

第三步,考察G的结构和几何解释(如图 6.2 所示). 由上知$G=\langle\sigma,\tau\rangle$,其中$\sigma^4=\tau^2=I,\tau\sigma=\sigma^3\tau$. G 是二面体群 D_8,用 $f(x)$ 的四个根来记正方形的四个顶点,则四边形的对称恰为一个根的置换,即为 Galois 群的一个元素. 因而 Galois 群 D_8 可看作是一个正方形的对称群.

第四步,确定 $G(E/Q)$ 的所有子群.

直接验证可知:阶为 8 的子群 $G\cong D_8$;

阶为 4 的子群

$G_1=\{I,\sigma^2,\sigma\tau,\sigma^3\tau\}\cong\mathbf{Z}_2\times\mathbf{Z}_2$;

阶为 2 的子群

$H_1=\{I,\sigma^2\tau\}\cong\mathbf{Z}_2,H_2=\{I,\tau\}\cong\mathbf{Z}_2,H_3=\{I,\sigma^2\}\cong\mathbf{Z}_2,H_4=\{I,\sigma\tau\}\cong\mathbf{Z}_2,H_5=\{I,\sigma^3\tau\}\cong\mathbf{Z}_2$;

阶为 1 的子群$\{I\}$.

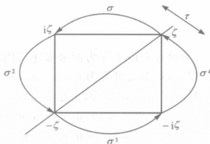


图 6.2

第五步,确定 $G(E/Q)$ 的所有子群之间的关系;

如图 6.3 所示,其中用上斜线连接 X 和 Y,表示 $X\subseteq Y$.

第六步,确定$G(E/Q)$的子群对应的E的子域之间的关系;由 Galois 理论的基本定理,$G(E/Q)$的子群对应的E的子域如图 6.4 所示,其中用上斜线连接X和Y,表示$X\subseteq Y$.

第七步,确定 E 与 Q 的中间域;

容易验证 Q 有三个二次扩域 $Q(\mathrm{i}),Q(\sqrt{2})$ 和 $Q(\sqrt{2}\mathrm{i})$,它们分别是三个四阶子群的固定域,即 $Q(\sqrt{2})=E^{G_1},Q(\mathrm{i})=E^{G_2},Q(\sqrt{2}\mathrm{i})=E^{G_3}$.

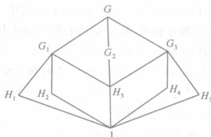


图 6.3

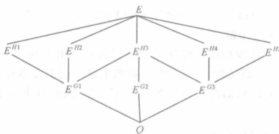


图 6.4

下面我们以 E^{H_4} 为例来描述其他的中间域.

E 的每个元可表为 $\alpha = a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 + a_4\mathrm{i} + a_5\omega\mathrm{i} + a_6\omega^2\mathrm{i} + a_7\omega^3\mathrm{i}$ 的形式,其中 $a_0,\cdots,a_7 \in Q$,于是

$$\begin{aligned}\sigma\tau(\alpha) &= a_0 + a_1\omega\mathrm{i} - a_2\omega^2 - a_3\omega^3\mathrm{i} - a_4\mathrm{i} + a_5\omega(-\mathrm{i})\mathrm{i} + a_6(\omega\mathrm{i})^2\mathrm{i} - a_7\mathrm{i}(\omega\mathrm{i})^3 \\ &= a_0 + a_5\omega - a_2\omega^2 - a_7\omega^3 - a_4\mathrm{i} + a_1\omega\mathrm{i} + a_6\omega^2\mathrm{i} - a_3\omega^3\mathrm{i}.\end{aligned}$$

因而 α 被 $\sigma\tau$ 固定当且仅当 $a_0 = a_0, a_1 = a_5, a_2 = -a_2, a_3 = -a_7, a_4 = -a_4, a_6 = a_6$,由此知

$$\alpha = a_0 + a_1(1+\mathrm{i}) + a_6/2((1+\mathrm{i})\omega)^2 - a_3/2((1+\mathrm{i})\omega)^3,$$

这意味着 $E^{H_4} = Q(\omega(1+i))$. 类似地我们有

$$E^{H_1} = Q(\omega\mathrm{i}), E^{H_2} = Q(\omega), E^{H_3} = Q(\omega^2,\mathrm{i}), E^{H_5} = Q(\omega(1-\mathrm{i})).$$

可以验证以上这些域就是所有的中间域,而且这些中间域之间的包含关系以及 Galois 理论的基本定理中的 5) 均成立.

第八步,确定 G 的正规子群与 Q 的 Galois 扩张.

验证可知 G 的全部正规子群为 G,G_1,G_2,C_3 和单位元群$\{I\}$. 由 Galois 理论的基本定理可知,

$Q = E^G, Q(\sqrt{2}) = E^{G_1}, Q(\mathrm{i}) = E^{G_2}, Q(\sqrt{2}\mathrm{i}) = E^{G_3}, Q(\sqrt{2}, \mathrm{i}) = E^{H_3}, E = E^1$ 是 Q 的含在 E 中的所有可能的 Galois 扩张.

事实上,Q 的这些扩张分别是多项式 $x, x^2 - 2, x^2 + 1, x^2 + 2, x^4 - x^2 - 2$ 以及 $x^4 - 2$ 在 Q 上的分裂域,因而都是 Q 的 Galois 扩张.

另一方面,$E^{H_2} = Q(\omega)$ 不是 Q 的 Galois 扩张,因为不可约多项式 $x^4 - 2$ 有一个根在 $Q(\omega)$ 中,但它不是 $x^4 - 2$ 的分裂域. 类似地,

$$E^{H_1} = Q(\omega\mathrm{i}), E^{H_4} = Q(\omega(1 + \mathrm{i})), E^{H_5} = Q(\omega(1 - \mathrm{i}))$$

均不是 Q 的 Galois 扩张.

第九步,确定含在 E 中的 Q 的 Galois 扩张的 Galois 群;

由上述讨论知,含在 E 中的 Q 的 Galois 扩张共有 6 个,其中 $G(E/Q) = G, G(E/E) = 1$,其他 4 个 Galois 扩张的 Galois 群也可由 Galois 基本定理得到,例如 $G(E/E^{H_3}) \cong G/H_3 \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

下面我们直接计算 $G(E/E^{H_3})$ 以说明它恰好是 $\mathbf{Z}_2 \times \mathbf{Z}_2$.

因为 $E^{H_3} = Q(\sqrt{2}, \mathrm{i})$,它的 Q 自同构完全由它在 i 和 $\sqrt{2}$ 上的作用确定. 易验证它恰有四个 Q 自同构,如下所示:

$I: \mathrm{i} \longmapsto \mathrm{i}, \sqrt{2} \longmapsto \sqrt{2}; f: \mathrm{i} \longmapsto \mathrm{i}, \sqrt{2} \longmapsto -\sqrt{2}$;

$g: \mathrm{i} \longmapsto -\mathrm{i}, \sqrt{2} \longmapsto \sqrt{2}; fg: \mathrm{i} \longmapsto -\mathrm{i}, \sqrt{2} \longmapsto -\sqrt{2}$.

因为 $f^2 = g^2 = I, fg = gf$,因而 $G(E/E^{H_3}) \cong \mathbf{Z}_2 \times \mathbf{Z}_2$,这恰是我们所希望的,直接计算其他几个子域来验证 Galois 理论的基本定理的 3).

第十步,确定 G 的共轭子群与 E 的共轭子域.

由于 $\sigma(Q(\omega)) = Q(\omega\mathrm{i})$,故 $\sigma(Q(\omega))$ 与 $Q(\omega\mathrm{i})$ 是共轭的,按照 Galois 理论的基本定理,其对应的 Galois 群 H_1 与 H_2 是共扼的,事实上,我们有 $H_1^\sigma = H_2$,类似地,$Q((1 + \mathrm{i})\omega)$ 与 $Q((1 - i)\omega)$ 是共轭的,群 $H_4^\tau = H_5$.

问题 6.2

1. 设 $f(x) = x^3 - 2 \in Q[x]$,计算 $f(x)$ 的 Galois 群.

2. 求证 $Q(\sqrt{2}, \sqrt{3}, \sqrt{5}))$ 是 Q 的 Galois 扩张,并求其 Galois 群.

3. 利用上题求

(1) $\sqrt{6} + \sqrt{10} + \sqrt{15}$ 在 Q 上的极小多项式;

(2) $\sqrt{2} + \sqrt{3}$ 在 $Q(\sqrt{6}, \sqrt{10}, \sqrt{15})$ 上的极小多项式.

4. 计算 $Q(\sqrt{2}, \sqrt{5})$ 在 Q 上的 Galois 群 G,找出 G 的全部子群及其对应的固定

域，找出 G 的全部正规子群及其对应的Galois扩张.

5. E/F 是有限Galois扩张，$F \subset K \subset E$，K 为中间域，若所有的中间域 K 对于 F 均有相同的次数，$[K : F]$，则 K/F 均为Galois扩张.

6. 设 F 是域，$f(x) \in F[x]$ 有一个根 $\alpha \in F$，求证：$f(x)$ 的Galois群与 $f(x)/(x-\alpha)$ 的Galois群是相同的.

§6.3 自同构群

经过Galois的研究，搞清楚了 $\mathbf{F}_i$ 与 $\mathbf{F}_{i-1}(i=1,2,\cdots,k)$ 的关系，其关键在于使 $\mathbf{F}_{i-1}$ 保持不变的 $\mathbf{F}_i$ 的自同构群的结构.这是Galois理论的核心内容.

前面已经给出了同构与自同构的概念，把它们应用到群、域上便可以得到群、域的同构与自同构：

定义 6.3.1 (1) 如果群 G 与 G' 间存在同构映射，则称群 G 与 G' 同构.群 G 到它自身的同构映射称为自同构.

(2) 设 $\mathbf{F}$ 与 $\mathbf{F}'$ 是两个域，$\mathbf{F}$ 与 $\mathbf{F}'$ 的代数运算分别记作 $+$、$\cdot$ 与 $\oplus$、$\odot$，如果对于 $\forall\ a,b \in \mathbf{F}$，总有 $f(a+b)=f(a)\oplus f(b)$，$f(a\cdot b)=f(a)\odot f(b)$，则称 $\mathbf{F}$ 到 $\mathbf{F}'$ 的一个双射 $f:\mathbf{F}\to\mathbf{F}'$ 为域 $\mathbf{F}$ 与 $\mathbf{F}'$ 间的同构映射，此时称 $\mathbf{F}$ 与 $\mathbf{F}'$ 同构；如果 f 是域 $\mathbf{F}$ 到它自身的同构映射，则称 f 是域 $\mathbf{F}$ 的自同构变换，简称自同构.

例 6.3.1 设 $\mathbf{F}(\sqrt{z})$ 是由数域 $\mathbf{F}$ 添 $\sqrt{z}$ 而生成的扩域，其中 $\sqrt{z}$ 是方程 $x^2-z=0$ 的一个正根，则对于 $\forall\ q_1=a+b\sqrt{z}\in\mathbf{F}(\sqrt{z})$，必存在 $q_2=a-b\sqrt{z}\in\mathbf{F}(\sqrt{z})$，求证：对于映射 f，使 $f(a+b\sqrt{z})=a-b\sqrt{z}$，那么 f 是 $\mathbf{F}(\sqrt{z})$ 的一个自同构.

证明 因为 $f(a+b\sqrt{z})=a-b\sqrt{z}$，显然 f 是满射，也是单射，因此是双射.对于 $\forall\ u,v\in\mathbf{F}(\sqrt{z})$，令 $u=a+b\sqrt{z}$，$v=c+d\sqrt{z}$，其中 $a,b,c,d\in\mathbf{F}$，则 $u+v=(a+c)+(b+d)\sqrt{z}$，所以 $f(u+v)=(a+c)-(b+d)\sqrt{z}$；又因为 $f(u)=a-b\sqrt{z}$，$f(v)=c-d\sqrt{z}$，所以 $f(u)+f(v)=(a+c)-(b+d)\sqrt{z}$.因此 $f(u+v)=f(u)+f(v)$.同理可证 $f(uv)=f(u)f(v)$.所以 f 是 $\mathbf{F}(\sqrt{z})$ 的自同构.

与置换的乘积相类似，也可以定义同一数域 $\mathbf{F}$ 上两个自同构变换 T_1 与 T_2 的乘积 $T_2\cdot T_1$ 为先作变换 T_1，再接着作变换 T_2.下面证明 $T_2\cdot T_1$ 是数域 $\mathbf{F}$ 上的自同构变换.

显然，$T_2\cdot T_1$ 是双射，并且对于 $\forall\ a,b\in\mathbf{F}$，有

$$T_2 \cdot T_1(a+b) = T_2(T_1(a+b)) = T_2(T_1(a) + T_2(T_1(b))$$
$$= T_2 \cdot T_1(a) + T_2 \cdot T_1(b).$$

同理可证 $T_2 \cdot T_1(ab) = (T_2 \cdot T_1(a)) \cdot (T_2 \cdot T_1(b))$.

所以 $T_2 \cdot T_1$ 是数域 F 上的自同构变换. **F** 上的恒等变换 I 显然是 **F** 上的自同构变换.

下面证明数域 **F** 上所有自同构变换构成的集合 G 关于上面定义的乘法运算作成一个群.

首先,两个自同构变换的乘积仍是数域 **F** 上的自同构变换,因此对所定义的乘法运算是封闭的,且结合律显然成立,又数域 **F** 的恒等变换是自同构变换,不难证明它是 G 的单位元,对于任意的自同构变换 $T \in G$,由于 T 是双射,所以 T^{-1} 显然存在,下面证明 T^{-1} 也是自同构变换,为此,对于数域 **F** 的任意二元素 a、b,设 $T^{-1}(a) = a'$,$T^{-1}(b) = b'$,则 $T(a') = a$,$T(b') = b$. 于是

$$T^{-1}(a+b) = T^{-1}(T(a') + T(b')) = T^{-1}(T(a'+b'))$$
$$= T^{-1}T(a'+b') = a' + b' = T^{-1}(a) + T^{-1}(b);$$
$$T^{-1}(ab) = T^{-1}(T(a')T(b')) = T^{-1}(T(a'b'))$$
$$= T^{-1} \cdot T(a'b') = a'b' = T^{-1}(a)T^{-1}(b).$$

所以 T^{-1} 也是自同构变换,即 $T^{-1} \in G$,即 G 对于上面定义的乘法作成群.

我们称数城 **F** 的全体自同构变换的集合 G 按照上面定义的乘法运算作成的群为数域 **F** 的自同构变换群,简称自同构群.

在上例中 $\mathbf{F}(\sqrt{z})$ 是由数域 **F** 添加 $\sqrt{z}$ 而生成的扩域,已证明了 f 是 $\mathbf{F}(\sqrt{z})$ 的自同构变换. 显然,把 f 连续施行两次,其结果不变,即 $ff = f^2 = I$. 所以 $\{I, f\}$ 就是 $\mathbf{F}(\sqrt{z})$ 的自同构变换群,且是周期为 2 的循环群. 由于对于 $\forall\, a \in F$,有 $f(a) = a$,所以在 f 的作用下 $\mathbf{F}(\sqrt{z})$ 中属于 **F** 的那些数保持不变,称这个群 $G = \{I, f\}$ 为数域 $\mathbf{F}(\sqrt{z})$ 的保持 **F** 不变的自同构变换群.

由于任何数域 **F** 包含有理数域 **Q**,设 T 是数域 **F** 的一个自同构变换,在 T 的作用下,任何有理数不变.

首先证明 $T(0) = 0$,为此取数 $a \in \mathbf{F}$,因为 $T(a+0) = T(a) + T(0)$,又由 $a + 0 = a$ 得 $T(a+0) = T(a)$,所以 $T(0) = 0$;

其次证明 $T(1) = 1$,取数 $b \in \mathbf{F}$,$b \neq 0$,因为 $T(b) = T(b \cdot 1) = T(b) \cdot T(1)$,由 $b \neq 0$ 且 $T(0) = 0$,知 $T(b) \neq 0$,所以 $T(1) = 1$;

再次证明对于任意自然数 n 有

$$T(n) = n \text{ 及 } T(-n) = -n,$$

$$T(n) = T(1+1+\cdots+1) = T(1)+T(1)\cdots+T(1)$$
$$= 1+1+\cdots+1 = n,$$

又 $n+(-n)=0$,所以 $T(n+(-n))=T(0)=0$. 但 $T(n+(-n))=T(n)+T(-n)=n+T(-n))$,所以 $T(-n)=-n$. 至此,已证明了在 T 的作用下任何整数保持不变.

最后证明在 T 的作用下,任意 $p/q(p,q$ 为任意整数,$q\neq 0)$ 保持不变,即 $T(p/q)=p/q$, 因为 $p=q(p/q)$,$T(p)=p$,$T(q)=q$,故有 $p=T(p)=T(q\cdot(p/q))=T(q)T(p/q)=q\,T(p/q)$,由此得 $T(p/q)=p/q$. 因此在自同构变换 T 作用下有理数不变.

一般地,如果 **K** 是 **F** 的扩域,记 **K** 的自同构变换群 G 中使 **F** 的元素不变的那些自同构变换的全体构成的集合为 H,容易证明 H 是 G 的子群,称 H 为数域 **K** 在其子域 **F** 上的自同构群.

群 H 使 **F** 的数不变,那么使域 **K** 的数如何变化?下面就回答这个问题.

定理 6.3.1　设数域 **K** 在其子域 **F** 上的自同构群 H,那么对于 $\forall\ T\in H, u\in \mathbf{K}$, $T(u)$ 必是 u 在 **F** 上的某一个共轭元素.

证明　只需证明 u 与 $T(u)$ 满足 **F** 上的同一个不可约方程.

设 u 满足 $x^n+b_{n-1}x^{n-1}+\cdots+b_1x+b_0=0$,其中 $b_{n-1},\cdots,b_1,b_0\in\mathbf{F}$,因为 $T\in H$,所以

$$\begin{aligned}0 = T(0) &= T(u^n+b_{n-1}u^{n-1}+\cdots+b_1u+b_0)\\ &= T(u^n)+T(b_{n-1}u^{n-1})+\cdots+T(b_1u)+T(b_0)\\ &= (T(u))^n+b_{n-1}T(u))^{n-1}+\cdots+b_1T(u)+b_0,\end{aligned}$$

所以 $T(u)$ 也满足 u 所满足的数域 **F** 上的不可约方程,即 $T(u)$ 是 u 在数域 **F** 上的某一个共轭元素.

例 6.3.2　$\mathbf{Q}(\sqrt{2})$ 是 **Q** 添加 $\sqrt{2}$ 生成的扩域,作 $\mathbf{Q}(\sqrt{2})$ 上的映射 $f:\mathbf{Q}(\sqrt{2})\to\mathbf{Q}(\sqrt{2})$,使 $f(a+b\sqrt{2})=a-b\sqrt{2}$,其中 $a,b\in\mathbf{Q}$,知 f 是自同构,且是保持 **Q** 中元素不变的自同构.

$f(\sqrt{2})=-\sqrt{2}$,$-\sqrt{2}$ 是 $\sqrt{2}$ 的共轭元素,因为它们同时满足 **Q** 上的不可约方程 $x^2-2=0$,因为 $f^2=I$,所以 $\mathbf{Q}(\sqrt{2})$ 在 **Q** 上的自同构群 $H=\{I,f\}$,它是一个周期为 2 的循环群.

另一方面,设 **F** 和 **K** 是两个数域,**K** 是 **F** 的扩域,$\mathbf{F}\subset\mathbf{K}$,**K** 在 **F** 上的自同构群 $H=\{S,I\}$ 则 $\mathbf{S}^2=I$,今证明 **K** 是 **F** 的二次扩域,对于 $\forall\ \alpha\in\mathbf{K}$,有 $S(\alpha)=\alpha'\in\mathbf{K}$,$\alpha$ 与 α' 可能不同,但 $\alpha+\alpha'$ 和 $\alpha\alpha'$ 在自同构 S 的作用下一定不变,

$$S(\alpha+\alpha')=S(\alpha)+S(\alpha')=\alpha'+\alpha=\alpha+\alpha';S(\alpha\alpha')=S(\alpha)S(\alpha')=\alpha\alpha'.$$

由于 S 是 $\mathbf{K}$ 在 $\mathbf{F}$ 上的自同构群 H 的元素，所以 $\alpha+\alpha'\in\mathbf{F}$，$\alpha\alpha'\in\mathbf{F}$，记 $\alpha+\alpha'=m$，$\alpha\alpha'=h$，则有 $m,h\in\mathbf{F}$，所以

$$\alpha\alpha''=\sqrt{h^2-4m},$$

于是 $\alpha=1/2h+\sqrt{h^2-4m}$，$\alpha'=1/2h-\sqrt{h^2-4m}$，

这就是说，α 必可表示为 $a+b\sqrt{q}$ 的形式，其中 $m,h\in\mathbf{F}$，从而 q 都是 $\mathbf{F}$ 中的数，这就说明数域 $\mathbf{K}$ 是由数域 $\mathbf{F}$ 添加由 $\mathbf{F}$ 中的数所确定的数 q 的平方根 $\sqrt{q}$ 生成的，由此可见 $\mathbf{K}$ 是 $\mathbf{F}$ 的二次扩域.

综上所述，$\mathbf{F}$ 上添加二次根式生成的正规扩域与保持 $\mathbf{F}$ 中数不变的 $\mathbf{K}$ 的自同构变换群有密切的联系.

例 6.3.3　$\mathbf{Q}$ 上不可约方程 $x^4-2x^2+9=0$ 的根域 $\mathbf{K}=\mathbf{Q}(\sqrt{2},\mathrm{i})$，显然有

$$\mathbf{Q}\subset\mathbf{Q}(\mathrm{i})\subset\mathbf{Q}(\sqrt{2},\mathrm{i})\text{ 和 }\mathbf{Q}\subset\mathbf{Q}(\sqrt{2})\subset\mathbf{Q}(\sqrt{2},\mathrm{i}).$$

$\pm\mathrm{i}$ 是 $\mathbf{Q}$ 上不可约方程 $x^2+1=0$ 的根，$\pm\sqrt{2}$ 是 $\mathbf{Q}$ 上不可约方程 $x^2-2=0$ 的根. $\mathbf{Q}(\sqrt{2},\mathrm{i})$ 上的任何元素都可以表示为 $a+b\sqrt{2}+c\mathrm{i}+d\mathrm{i}\sqrt{2}$，其中 $a,b,c,d\in\mathbf{Q}$，$\mathbf{Q}(\sqrt{2},\mathrm{i})$ 上的一个自同构变换，

$$S:S(a+b\sqrt{2}+c\mathrm{i}+d\mathrm{i}\sqrt{2})=a-b\sqrt{2}+c\mathrm{i}-d\mathrm{i}\sqrt{2},$$

显然 S 保持 $\mathbf{Q}(\mathrm{i})$ 中的数不变，$\mathbf{Q}(\sqrt{2},\mathrm{i})$ 上的另一个自同构变换，

$$T:T(a+b\sqrt{2}+c\mathrm{i}+d\mathrm{i}\sqrt{2})=a+b\sqrt{2}-c\mathrm{i}-d\mathrm{i}\sqrt{2},$$

显然 T 保持 $\mathbf{Q}(\sqrt{2})$ 中的数不变，而 TS 也是 $\mathbf{Q}(\sqrt{2},\mathrm{i})$ 的一个自同构变换.

因此 $\mathbf{Q}(\sqrt{2},\mathrm{i})$ 在 $\mathbf{Q}$ 上的自同构群 $H=\{I,S,T,TS\}$，不难证明 $T^2=S^2=I$，$TS=ST$，$(ST)(ST)=I$，并且 $\mathbf{Q}(\sqrt{2},\mathrm{i})$ 在 $\mathbf{Q}(\sqrt{2})$ 上的自同构群是 $\{I,T\}$，在 $\mathbf{Q}(\mathrm{i})$ 上的自同构群是 $\{1,S\}$. $\mathbf{Q}(\sqrt{2})$ 与 $\mathbf{Q}\{\mathrm{i}\}$ 是 $\mathbf{Q}$ 与 $\mathbf{Q}(\sqrt{2},\mathrm{i})$ 的中间扩域. 这个例子说明，不同的中间扩域相应于不同的自同构群.

§6.4　方程有根式解的判别方法

方程论中一个古典的问题是：给了一个数域 F 上的一元 n 次方程 $f(x)=0$，是否存在一个由 $f(x)$ 的系数的有限次加、减、乘、除及开方运算组成的公式，使得这个方程的每个根都可由这个公式表达出来？

对于一元二次方程 $ax^2+bx+c=0$，$a\neq0$，我们有解的公式：

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}.$$

类似地，对于一元三次、四次方程，我们也有相应的解的公式. Galois 理论就是研究五次及五次以上的一元方程是否有类似的公式解.

对于 $f(x)\in F[x]$，首先假设有这样一个公式存在，由于加、减、乘、除运算可在 F 中进行，而对一个数 a 开 n 次方相当于求一个数 α 使得 $\alpha^n=a$，因此存在一个子域链 $F=F_0\subseteq F_1\subseteq F_2\subseteq\cdots\subseteq F_k=E$，其中 $F_i=F_{i-1}(\alpha_i)$，$(\alpha_i)^{n_i}\in F_{i-1}(1\leqslant i\leqslant k)$，使得 $f(x)$ 的每个根都在 E 内.

反之，如果存在 F 的扩域链，使得 $f(x)$ 的每个根都含在 E 内，则对方 $f(x)=0$ 的每个根，一定存在它的一个表达式，这个表达式是由 $f(x)=0$ 的系数经有限次加、减、乘、除及开方运算组成的，此时我们说 $f(x)$ 的根有根式表示.

定义 6.4.1　域的扩张 E/F 称为纯根式扩张，若存在自然数 $n,\omega\in E$，使得 $\omega^n\in F$ 且 $E=F(\omega)$，E/F 称为根式扩张，若存在纯根式扩张链 $F=E_0\subseteq E_1\subseteq E_2\subseteq\cdots\subseteq E_h=E$，使得每个 E_{i+1}/E_i 是纯根式扩张.

设 E 是 F 上多项式 $f(x)$ 的分裂域，$f(x)$ 称为根式可解(或有根式解)，若存在一个纯根式扩张链 $F=E_0\subseteq E_1\subseteq E_2\subseteq\cdots\subseteq E_h$ 使得 $E\subseteq E_h$.

引理 6.4.1　设 F 是域，$E=F(\alpha_1\cdots\alpha_n)$ 是 F 的扩域，若 $\sigma\in G(E/F)$，且对所有的 i 都有 $\sigma(\alpha_i)=\alpha_i$，则 $\sigma=1_E$.

证明　对 n 用归纳法. 若 $n=1$，则对每个 $\omega\in E,\omega=f(\alpha_1)/g(\alpha_1)$，其中 $f(x)$，$g(x)\in F[x]$ 且 $g(\alpha_1)\neq 0$，因为 σ 固定 α_1 以及 $f(x)$ 和 $g(x)$ 的系数，故 σ 固定所有 $\omega\in E$，且对于 $n=k-1$，由归纳假设，σ 固定 $K=F(\alpha_1\cdots\alpha_{k-1})$ 中每个元，令 $K_1=K(\alpha_k)$，由于 σ 固定 α_k 以及 K，重复上述作法，即得 σ 固定所有的 $\omega\in K_1$，结论得证.

引理 6.4.2　设 m 是正整数，F 是域，$\mathrm{char}F=0$ 或 $\mathrm{char}F$ 不整除 m，E 是 F 上多项式 x^m-1 的分裂域，则 $G(E/F)$ 是 d 阶循环群，其中 $d|m$.

证明　设 $\mathrm{char}F$ 不整除 m，则 $mx^{m-1}\neq 0$，因而 $(f(x),f'(x))=1$，则 $f(x)$ 无重根. 因而 E 含有 m 个不同的 m 次单位根，易知这 m 个 m 次单位根作成 E 的乘群 E^* 的一个子群 W_m，它是 m 阶的循环群，因而它有一个 m 次本原单位根. 设其中的一个本原单位根为 ω，于是 $E=F(\omega)$. 设 $\sigma\in G(E/F)$，则对某个 $1\leqslant i\leqslant m,\sigma(\omega)=\omega^i$，考虑 $G(E/F)$ 到 W_m 的映射

$$\varphi:\sigma\longmapsto\omega^i,$$

若 $\sigma(\omega)=\omega^i$，

则 φ 是群的单同态，故 $G(E/F)$ 是 d 阶循环群，其中 $d|m$.

推论 6.4.3　设 m 是正整数，F 是域，$\mathrm{char}F=0$ 或 $\mathrm{char}F$ 不整除 m. 若 E 是 F 上多

项式 $x^m - b(0 \neq b \in F)$ 的分裂域，且 F 含有一个 m 次本原单位根 ζ，则 E 是 F 纯根式扩张且 $G(E/F)$ 是 d 阶循环群，其中 $d|m$.

证明　设 $\alpha \in E$ 是 $x^m - b$ 的一个根，则 $\alpha, \alpha\zeta, \cdots, \alpha\zeta^{m-1}$ 是 $x^m - b$ 在 E 中的 m 个不同的根，故 $E = F(\alpha)$ 且 $\alpha^m = b \in F$，从而 E 是 F 的纯根式扩张，由类似于命题 6.2.2 的证明可知 G 是 d 阶循环群，其中 $d|m$.

引理 6.4.4　设 E 是域 F 上多项式 $f(x)$ 的分裂域，若 F^* 是 F 的扩域，E^* 是 $f(x)$ 在 F^* 上的分裂域，则 $\varphi: \sigma \longmapsto \sigma|_E$ 是 $G(E^*/F^*)$ 到 $G(E/F)$ 的单同态.

证明　设 $f(x)$ 在 E 中的根为 $\alpha_1, \cdots, \alpha_n$，则 $E = F(\alpha_1 \cdots \alpha_n)$，$E^* = F^*(\alpha_1 \cdots \alpha_n)$，显然有 $F \subseteq E \subseteq E^*$，对于 $\forall\, \sigma \in G(E^*/F^*)$，因为 σ 置换 $f(x)$ 的根，故 $\sigma|_E \in G(E/F)$. 直接验证可知 φ 是一个群同态. 又

$$\sigma \in \mathrm{Ker}\varphi \Leftrightarrow \sigma|_E = 1 \Leftrightarrow \sigma(\alpha_i) = \alpha_i (1 \leqslant i \leqslant n) \Leftrightarrow \sigma = 1,$$

因此 $\mathrm{Ker}\varphi = 1$，即 φ 为单同态.

引理 6.4.5　设 p 为素数，E 是 F 的 p 次 Galois 扩张，若 F 含有一个 p 次本原单位根 ω，则 $E = F(\alpha)$，其中 $\alpha^p \in F$.

证明　因为 E/F 是 p 次 Galois 扩张，故它的 Galois 群 $G = G(E/F)$ 是 p 阶循环群. 设 $G = (\sigma)$，把 E 看作 F 上的向量空间，因为 $\sigma \in G(E/F)$，故对于任意的 $a \in F$，$u \in E$，我们有 $\sigma(au) = \sigma(a)\sigma(u) = a\sigma(u)$，因而 σ 可看作 E 的一个线性变换. 因为 σ 是 p 阶元，故 $\sigma^p = 1_E$，从而 σ 的特征值是 p 次单位根. 因为 $\sigma \neq 1_E$，故对于 σ 的某个特征向量 $\alpha \in E$，存在一个不等于 1 的 n 次本原单位根 ω 使得 $\sigma(\alpha) = \omega\alpha$，于是 $\alpha \notin F$，又 $\sigma(\alpha^p) = \omega^p\alpha^p = \alpha^p$，由此 $\alpha^p \in E^G = F$. 有 $p = [E:F] = [E:F(\alpha)][F(\alpha):F]$，因为$[F(\alpha):F] \neq 1$，故$[E:F(\alpha)] = 1$，也即 $E = F(\alpha)$.

定理 6.4.6　设 F 是域，$f(x) \in F[x]$ 是 $n(\geqslant 1)$ 次可分多项式，E 是 $f(x)$ 在 F 上的分裂域，则 $G(E/F)$ 同构于 n 次对称群 S_n 的一个子群.

证明　设 $W = \{\alpha_1, \cdots, \alpha_n\}$ 是 $f(x)$ 的 n 个不同的根组成的集合，对于 $\sigma \in G(E/F)$，知 $\sigma|_W$ 是 W 的一个置换，即 $\sigma|_W \in S_W \cong S_n$，令 $\varphi: \sigma \longmapsto \sigma|_W$ 是 $G(E/F)$ 到 S_n 的映射；对 $\forall\, \sigma, \tau \in G(E/F)$，$\varphi((\sigma\tau)(\alpha_i) = (\sigma\tau)|_W(\alpha_i) = (\sigma\tau)(\alpha_i) = \sigma(\tau(\alpha_i) = \sigma(\tau|_W(\alpha_i)) = \sigma|_W(\tau|_W(\alpha_i)) = \varphi(\sigma)\varphi(\tau)(\alpha_i)$，故 $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$，$\varphi$ 是同态；若 $\sigma \in \mathrm{Ker}\varphi$，则 $\sigma|_W(\alpha_i) = \alpha_i$(对 $\forall\, i$). 又 σ 也固定 F，所以 $\sigma = 1_E$，即 $\mathrm{Ker}\varphi = 1$，故 φ 是单射.

定理 6.4.7　设 F 是域，$p(x)$ 是 $F[x]$ 的可分多项式，E 是 $p(x)$ 在 F 上的分裂域，则 $p(x)$ 是不可约的当且仅当 $G(E/F)$ 是 $p(x)$ 的零点组成的集合上的传递群，即 $G(E/F)$ 传递地作用在 $p(x)$ 的零点组成的集合上.

证明　设 $p(x)$ 是不可约的，$\alpha, \beta \in E$，E 是 $p(x)$ 的根，则存在 $F(\alpha)$ 到 $F(\beta)$ 的同构 φ 使得 $\varphi(\alpha) = \beta$，且固定 F. 又知 φ 可扩展为 E 的一个自同构 Φ 使得 Φ 固定 F，也即

$\Phi \in G(E/F)$. 现在有 $\Phi(\alpha)=\varphi(\alpha)=\beta$,故 $G(E/F)$ 传递地作用在 $p(x)$ 的根集(零点组成的集合)上.

反之,设 $G(E/F)$ 传递地作用在 $p(x)$ 的根集上,若 $p(x)$ 可约,设 $p(x)=p_1(x)p_2(x)\cdots p_k(x)$,其中 $p_i(x)\in F[x]$ 是不可约的,$k\geqslant 2$. 在 E 中选择 $p_1(x)$ 的一个根 α,选择 $p_2(x)$ 的一个根 β,由假设存在 $\sigma\in G(E/F)$ 使得 $\sigma(\alpha)=\beta$,由命题 6.6.2 知,σ 置换 $p(x)$ 的根. 又因为 $p(x)$ 无重根,故 β 不能是 $p_1(x)$ 的根,矛盾. 故 $k=1$,即 $p(x)$ 是不可约的.

定理 6.4.8　设 K 是 F 的有限可分扩域,则存在 K 的扩域 E 使得 E 是 $F[x]$ 中某个多项式 $f(x)$ 的分裂域. 若 K/F 是根式扩张,则 E/F 也是根式扩张.

证明　设 $K=F(\alpha_1\cdots\alpha_n)$,则对每个 α_i,存在 F 上唯一的不可约多项式为 $p_i(x)$ 使得 $p_i(\alpha_i)=0$. 令 E 是 $f(x)=p_1(x)\cdots p_n(x)$ 在 F 上的分裂域,则 $K\subseteq E$.

另一方面,若 α_1,α_2 是 $p_i(x)$ 的两个根,存在 $F(\alpha_1)$ 到 $F(\alpha_2)$ 的同构映射 ψ 使得 $\psi(\alpha_1)=\alpha_2$,这样的 ψ 可扩展为 E 的自同构 $\sigma\in G=G(E/F)$ 使得 $\sigma(\alpha_1)=\psi(\alpha_1)=\alpha_2$,

又知若 α_i 是 $f(x)$ 的一个根,则对任意的 $\sigma\in G,\sigma(\alpha_i)\in\sigma(K)$ 也是 $f(x)$ 的根,从而 E 由 $\{\sigma(K)\mid\sigma\in G\}$ 生成,其中 $\sigma(K)=F(\sigma(\alpha_1)\cdots\sigma(\alpha_n))$. 设 K/F 是根式扩张,不妨设

$$F\subseteq F(\gamma_1)\subseteq F(\gamma_1,\gamma_2)\subseteq\cdots\subseteq F(\gamma_1,\gamma_2\cdots\gamma_t)=K$$

其中每个 $F(\gamma_1,\gamma_2\cdots\gamma_{i+1})$ 是 $F(\gamma_1,\gamma_2\cdots\gamma_i)$ 的纯根式扩张,于是对于每个 $\sigma\in G,\sigma(K)=F(\sigma(\gamma_1)\cdots\sigma(\gamma_t))$,是 F 的根式扩张. 下证 E 是 F 的根式扩张,令 $M_1=\{\sigma(\gamma_1)\mid\sigma\in G\}$,把 M_1 中的元添加到 F 中,得到 F 的一个扩域 K_1,设 $G=\{1,\sigma,\tau,\cdots\}$,则我们有下列纯根式扩张链

$$F\subseteq F(\gamma_1)\subseteq F(\gamma_1,\sigma(\gamma_1))\subseteq F(\gamma_1,\sigma(\gamma_1),\tau(\gamma_1))\subseteq\cdots\subseteq K_1$$

例如,若 $\gamma_1^m\in F$,则 $\tau(\gamma_1^m)=\tau(\gamma_1)^m\in\tau(F)=F$,因而 $\tau(\gamma_1)^m\in F\subseteq F(\gamma_1,\sigma(\gamma_1))$. 假设对所有的 $j\leqslant i$,包含 $M_i=\{\sigma(\gamma_i)\mid\sigma\in G\}$ 中所有元的根式扩张 K_i/F 已构造出来,令 $M_{i+1}=\{\sigma(\gamma_{i+1})\mid\sigma\in G\}$,类似于上述作法,把 M_{i+1} 中的元添加到 K_i 中,得到 K_i 的一个扩域 K_{i+1},显而易见 K_{i+1}/K_i 是根式扩张.

例如,若 $\gamma_{i+1}^m\in F(\gamma_1,\gamma_2\cdots\gamma_i)$,则 $\tau(\gamma_{i+1})\in F(\tau(\gamma_1)\cdots\tau(\gamma_i))\subseteq K_i$,由此可知 K_{i+1} 是 F 的根式扩张. 由归纳原理知,因为 $E=K_t$,故 E 是 F 的根式扩张.

定理 6.4.9　设 F 是特征为零的域,则 F 上多项式有根式解当且仅当 F 上多项式的 Galois 群是可解群.

证明　$\Rightarrow$ 设 F 上多项式 $f(x)$ 有根式解,则存在一个纯根式扩张链

$$F=E_0\subseteq E_1\subseteq\cdots\subseteq E_h=K$$

使得 $E\subseteq K$,其中 E 是 $f(x)$ 在 F 上的分裂域,设 $E_{i+1}=E_i(\omega_i)$,$\omega_i^n=u_i\in E_i$,由定理

6.4.8 可设 K 是 F 的 Galois 扩张，设 $G=G(E/F)$ 是 $f(x)$ 在 F 上的 Galois 群，由 Galois 基本定理，$G(E/F)\cong G(K/F)/G(K/E)$. 只需证 $G(K/F)$ 可解即可.

令 $n=n_1n_2\cdots n_t$，令 M 是 x^n-1 在 K 上的分裂域，知 M 有一个 n 次本原单位根 ζ，可以看出，所有的 $n_i(1\leqslant i\leqslant t)$ 次单位根均在 $F(\zeta)$ 中，因为 K 是 F 的 Galois 扩张，故它是 F 上某个多项式 $g(x)$ 的分裂域. 设 M 是多项式 $(x^n-1)g(x)$ 在 F 上的分裂域，故 M 也是 F 上的 Galois 扩张，因为 $F\subseteq K\subseteq M$，再由 Galois 基本定理，

$$G(K/F)\cong G(M/F)/G(M/K),$$

因而只需证 $G(M/F)$ 可解即可.

令 $M_0=F, M_1=F(\zeta), M_2=M_1(\omega_1),\cdots,M_{t+1}=M(\omega_t)=M$，

因为所有的 n_i 次本原单位根均在 $M_1=F(\zeta)$ 中，从而都在 M_i 中，故在 $i=0$ 之后 M_{i+1} 是 M_i 的分裂域，因而 M_{i+1} 是 M_i 的 Galois 扩张. 令 $H_i=G(M/M_i)$，则 $H_0=G(M/F)$，$H_{t+1}=1$.

于是我们得到 $G(M/F)$ 的子群列

$$H_0\supseteq H_1\supseteq\cdots\supseteq H_{t+1}=1.$$

因为 M 是 M_i 上的 Galois 扩张，M_{i+1} 是 M_i 上的 Galois 扩张，由 Galois 理论的基本定理知

$$G(M/M_{i+1})=H_{i+1}\lhd G(M/M_i)=H_i，且\ H_i/H_{i+1}\cong G(M_{i+1}/M_i),$$

则对 $\forall\, i$，H_i/H_{i+1} 是循环群，知 $G(M/F)$ 是可解群.

$\Leftarrow$ 设 E 是 $f(x)$ 在 F 上的分裂域，$f(x)$ 的 Galois 群 $G=G(E/F)$ 是可解群，则 G 有一个指数为素数 p 的正规子群 H，设 ω 是一个 p 次本原单位根. 因为 F 的特征为零，故 ω 含在 F 的某个扩域 F^* 中，我们对 $[E:F]$ 用归纳法.

若 $F=E$，结论显然成立，此时 E 是它自身的根式扩张域. 考虑中间域 $F<E^H<E$，因为 E/F 是 Galois 扩张，故 E/E^H 也是 Galois 扩张. 由 Galois 理论的基本定理知 $G(E/E^H)$ 也是可解群. 因为 $[E:E^H]<[E:F]$，由归纳假设，存在一个纯根式扩张链

$$E^H\subseteq E_1\subseteq\cdots\subseteq E_t,$$

其中 $E\subseteq E_t$，因为 $H\lhd G$，又由 Galois 理论的基本定理知，E^H/F 是 Galois 扩张，且

$$[G:H]=p=[E:E^H].$$

我们分两种情况讨论.

1) $\omega\in F$. 在这种情况下，$E^H=F(\alpha)$，其中 $\alpha^p\in F$，因而上述纯根式扩张链可以通过添加 $F\subseteq E^H$ 加长而得到 E_t/F 是一个根式扩张.

2) $\omega\notin F$. 令 $F^*=F(\omega)$，设 $E^*=E(\omega)$，因为 E 是 $f(x)$ 在 F 上的分裂域，故 E^* 是 $f(x)(x^p-1)$ 在 F 上的分裂域. 由于 $\mathrm{char}F=0$，故 x^p-1 是可分多项式，由定理 4.1.4 知 E^*/F 是 Galois 扩张，从而 E^*/F^* 也是 Galois 扩张. 设 $G^*=G(E^*/F^*)$，则存

在一个 G^* 到 G 的单同态，于是 G^* 也是可解群.

因为 $\omega \in F^*$，这归纳为情形 1)，从而存在纯根式扩张链

$$F^* \subseteq E_1^* \subseteq \cdots \subseteq E_m^*，其中 E \subseteq E^* \subseteq E_m^*，$$

又 $F^* = F(\omega)$，故这个纯根式扩张链可以通过添加 $F \subseteq F^*$ 加长而得到 E_m^*/F 的一个根式扩张，由归纳原理，结论成立.

推论 6.4.10　设 F 是特征为零的域，则次数 $\leqslant 4$ 的 F 上多项式 $f(x)$ 都有根式解.

证明　设 G 是 $f(x)$ 的 Galois 群，则 G 同构于 S_4 的一个子群，但 S_4 是可解群，从而 G 是可解的，即 $f(x)$ 有根式解. 对于 5 次以上的多项式，有些有根式解，有些则没有.

例 6.4.11　Q 上的多项式 $x^5 - 1$ 有根式解，因为若 ζ 是一个 5 次本原单位根，则 $Q(\zeta)$ 是 $x^5 - 1$ 的分裂域，又它的 Galois 群是循环群，从而有根式解.

例 6.4.12　Q 上的多项式 $x^5 - 6x + 3$ 没有根式解. 下面我们对此进行证明.

由 Eisenstein(艾森斯坦因) 判别法知，$f(x) = x^5 - 6x + 3$ 在 $\mathbf{Q}$ 上不可约，因而 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域 E 上的次数被 5 整除，从而 5 整除 $|G|$，其中 $G = G(E/\mathbf{Q})$ 同构于 S_5 的一个子群，因为 S_5 中阶为 5 的元只能是 5 轮换，故 G 含有一个 5 轮换，不妨设为 (12345)，通过计算得，$f(-2) = -17$，$f(0) = 3$，$f(1) = -2$，$f(2) = 23$. 由此可知 $f(x)$ 至少有三个实根. 若 $f(x)$ 有 4 个实根，则 $f'(x) = 5x^4 - 6$ 将至少有 3 次为零，这不可能，因而 $f(x)$ 恰有 3 个实根，又由代数基本定理，$f(x)$ 恰有两个非实根. 设 τ 是复数域 $\mathbf{C}$ 上的共轭自同构，则 τ 互换这两个非实根，而固定另外 3 个实根，故 $\tau|_E \in G$ 是一个对换，不妨设为 (1,2). 现在 G 含有一个 5 轮换 (1,2,3,4,5) 和一个对换 (1,2). 考虑 $\langle (1,2,3,4,5),(1,2) \rangle$，计算 (1,2) 被 (1,2,3,4,5) 的共轭，利用 $S_5 = \{(1\ i) \mid i = (2,3,4,5)\}$，易知 $G \cong S_5$，因为 S_5 不是可解群，所以没有根式解.

推论 6.4.11　设 K 是特征为零的域，则 K 上 $n(\geqslant 5)$ 次一般多项式没有根式解.

证明　设 $f(x) = (x - y_1)\cdots(x - y_n)$ 是 K 上的 n 次一般多项式，设 $E = K(y_1 \cdots y_n)$，$F = K(a_0 a_1 \cdots a_{n-1})$，其中 a_i 是关于 $y_1 \cdots y_n$ 的初等对称多项式，则 E 是 $f(x)$ 在 F 上的分裂域.

首先我们证明 $G(E/F) \cong S_n$. 设 $\sigma \in S_n$，令

$$\bar{\sigma}: f(y_1 \cdots y_n) \longmapsto f(y_{\sigma(1)} \cdots y_{\sigma(n)}),$$

通过验证可知 $\bar{\sigma}$ 是 $K[y_1 \cdots y_n]$ 的一个自同构，因为 E 是 $K[y_1 \cdots y_n]$ 的商域，则以明显的方法 $\bar{\sigma}$ 可扩展为 E 的自同构 σ^*，又由 F 的作法知 σ^* 固定 F，从而 $\sigma^* \in G(E/F)$. 易验证 $\sigma \longmapsto \sigma^*$ 是 S_n 到 $G(E/F)$ 的单射. 从而

$$|S_n| \leqslant |G(E/F)|，又 |G(E/F)| \leqslant |S_n|，故 G(E/F) \cong S_n.$$

从以上讨论看出，有的 $n(\geqslant 5)$ 次方程有根式解，有的没有根式解，这完全取决于方程的 Galois 群是否为可解群，因而 Galois 群的计算是十分重要的，但它一般是非常困难

的，目前 Galois 理论领域研究内容之一就是计算有理数域 $\mathbf{Q}$ 上小次数的多项式的 Galois 群.

Galois 理论中一个有趣的称为逆 Galois 问题是：对每一个有限群 G，是否存在 $\mathbf{Q}$ 上的 Galois 扩张 E，使得 $G(E/\mathbf{Q})=G$? 从目前结果来看，我们对这个问题的回答都是肯定的. 已经知道下列群是 $\mathbf{Q}$ 上的 Galois 扩张 E 的 Galois 群：$A_n, S_n, PSL(2,p)$（p 为素数），可解群. 有限单群分类完成之后，已知大多数单群都是 Galois 群.

问题 6.4

1. 确定下列多项式的 Galois 群.

1) $f_1(x)=x^3-x^2+4$；

2) $f_2(x)=x^3-2x^2+4$；

3) $f_3(x)=x^3-x+1$；

4) $f_4(x)=x^3+x^2-2x-1$；

5) $f_5(x)=x^3-10x^2+1$.

2. 设 $f(x)$ 是 $\mathbf{Q}[x]$ 的 p 次不可约多项式，p 为素数，若 $f(x)$ 恰有两个复根，则 $f(x)$ 在 $\mathbf{Q}$ 上的 Galois 群是 S_p. 举例说明，如果 p 不是素数，结论不一定成立.

3. 利用上题证明 x^5-2x^3-8x+2, x^5-4x+2 没有根式解.

4. 设 F 是特征为零的域，$f(x)\in F[x]$ 是 5 次多项式，其分裂域为 E，求证：$f(x)$ 有根式解当且仅当 $[E:F]\leqslant 60$.

5. 证明：对有限群 G，存在 Galois 扩张 E/F 使得 $G(E/F)\cong G$.

6. 设 $f(x)$ 是域 F 上的不可约多项式，若它有一个根可用根式表示，则它所有的根都可用根式表示.

§6.5　Galois 群与用根号解代数方程

定义 6.5.1　设 $f(x)=0$ 是数域 $\mathbf{F}$ 上的方程，数域 $\mathbf{N}$ 是 $f(x)=0$ 的根域，则称 $\mathbf{N}$ 在 $\mathbf{F}$ 上的自同构群为方程 $f(x)=0$ 的 Galois 群.

已知 $\mathbf{Q}$ 上的方程 $x^4-2x^2+9=0$ 的根域 $\mathbf{N}=\mathbf{Q}(\sqrt{2},i)$，而 $\mathbf{Q}(\sqrt{2},i)$ 在 $\mathbf{Q}$ 上的自同构群是 $\{I,S,T,TS\}$，因此，$\mathbf{Q}$ 上的方程 $x^4-2x^2+9=0$ 的 Galois 群是 $\{I,S,T,TS\}$，其中 $T^2=S^2=I, TS=ST, ST\cdot ST=SSTT=I$.

定理 6.5.1　设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ 是数域 $\mathbf{F}$ 上的不可约多项式，在根域 $\mathbf{N}$ 内有 n 个不同的根，则 $f(x)=0$ 的 Galois 群是 $n!$ 个置换构成的对称群 S_n.

证明　设 $u_1, u_2 \cdots u_n$ 是方程 $f(x)=0$ 的 n 个不同的根，知 $\mathbf{N}$ 是 $\mathbf{F}$ 的正规扩域. 又 $\mathbf{N}$ 在 $\mathbf{F}$ 上的自同构群的任意元素 T，必把根变成其共轭数 u_j，而且不同的根所对应的共轭数也不同，因此 T 相当于 $u_1 u_2 \cdots u_n$ 的一种排列，即为置换.

另一方面，由根域的定义知 $\mathbf{N}$ 中的任一数 u 必可表示为系数属于 $\mathbf{F}$ 的 $u_i, u_i \cdots tu_i$ 的多项式：

$$\omega = h(u_1 u_2 \cdots u_n).$$

因为 $\mathbf{F}$ 中的数在 T 的作用下不变，所以

$$T(\omega) = T(h(u_1 u_2 \cdots u_n)) = h(T(u_1), T(u_2) \cdots T(u_n))$$
$$= h(u_{i_1}, u_{i_2} \cdots u_{i_n}).$$

所以 T 在 ω 上的作用，完全由 T 在 $u_1 u_2 \cdots u_n$ 上的作用，即 $T(u_i) = u_{j_i}$，$i = 1, 2 \cdots n$ 这一置换所唯一确定. 综上所述，自同构变换 f 和置换 T 可看成是相同的变换.

下面讨论本节的中心问题：怎样的方程才可以用代数方法.

定理 6.5.2　　$\mathbf{F} = \mathbf{Q}(\alpha_1, \alpha_2 \cdots \alpha)$ 上的代数方程：$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$ 的 Galois 群为可解群 $\Leftrightarrow$ 方程可用代数方法求解.

我们知道，一个方程能用代数方法求解等价于它的根域 $\mathbf{N}$ 可由 $\mathbf{F}$ 经过有限次添加根式生成，每次添加根式生成的扩域 $\mathbf{K}$，形成一列插在 $\mathbf{F}$ 与 $\mathbf{N}$ 之间的中间域：

$$\mathbf{F} = \mathbf{K}_0 \subset \mathbf{K}_1 \subset \mathbf{K}_2 \subset \cdots \subset \mathbf{K}_s = \mathbf{N}, \qquad (*)$$

$\mathbf{K}_{i+1}$ 是由 $\mathbf{K}_i$ 添加 $x^{r_i} - \alpha_i = 0$ 的根（$\alpha_i \in \mathbf{K}$，r_i 是素数）生成的扩域，可以证明，数 1 的任意次根总可由有理数经有限次加、减、乘、除及开方运算求得，因此不妨先把 1 的所有各次方根添加到 $\mathbf{F}$ 中而生成一扩域，为简单起见仍记此扩域为 $\mathbf{F}$，即不妨设 $\mathbf{F}$ 是包含方程系数及 1 的各次根的最小数域，显然，这并不影响方程能否用代数方法求解的讨论.

方程 $x^{r_i} - \alpha_i = 0$ 的根，除了 $\alpha_i^{\frac{1}{r_i}}$，还有 $\omega\alpha_i^{\frac{1}{r_i}}, \omega^2\alpha_i^{\frac{1}{r_i}}, \cdots, \omega^{r_i-1}\alpha_i^{\frac{1}{r_i}}$，其中 ω 是 1 的 r_i 次原根，这些与 $\alpha_i^{\frac{1}{r_i}}$ 共轭的根也都属于 $\mathbf{K}_{i+1}$（因为 ω 属于 $\mathbf{F}$），因此 $\mathbf{K}_{i+1}$ 是 $\mathbf{K}_i$ 上的方程 $x^{r_i} - \alpha_i = 0$ 的根域，从而是 $\mathbf{K}_i$ 的正规扩域，所以上面的一列扩域 $\mathbf{K}_1, \mathbf{K}_2, \cdots, \mathbf{K}_s$ 都是正规扩域，并且

$$[\mathbf{K}_1 : \mathbf{F}] = \mathbf{r}_1, [\mathbf{K}_2 : \mathbf{K}_1] = r_2, \cdots, [K_s : K_{s-1}] = [\mathbf{N} : K_{s-1}] = r_s \text{ 都是素数}.$$

下面根据正规扩域序列（*）分析 $\mathbf{N}$ 在 $\mathbf{F}$ 上的自同构群（即方程的 Galois 群 G 的结构）. 由于 $\mathbf{F} \subset \mathbf{K}_1 \subset \mathbf{N}$，所以使 $\mathbf{K}_1$ 中的数不变的 $\mathbf{N}$ 的自同构变换当然也使 $\mathbf{F}$ 中的数不变，故 $\mathbf{N}$ 在 $\mathbf{K}_1$ 上的自同构群 G_1 是 G 的子群，而且由于 $\mathbf{K}_1$ 是 $\mathbf{F}$ 的正规扩域，可以证明 G_1 一定是 G 的不变子群，并且（G 的阶数）：（G_1 的阶数）$= [\mathbf{K}_1 : \mathbf{F}] = r_1$.

同理，域 $\mathbf{N}$ 在 $\mathbf{K}_i$ 上的自同构群 G_i 是 G_{i-1} 的不变子群，并且（G_{i-1} 的阶数）：（G_i 的阶

数) $= [\mathbf{K}_i:\mathbf{K}_{i-1}]r_i, i = 1, 2 \cdots s$,所以由正规扩域序列(*)得出Galois群的不变子群序列

$$G \supset G_1 \supset G_2 \supset \cdots G_s = I,$$

并且由于 $r_1, r_2, \cdots, r_s$都是素数,所以 G_i 都是 G_{i-1} 的极大不变子群. 所以上式是合成群列,$r_1,$, r_2, $\cdots r_s$ 是组合因数. 因此,当一个方程可用代数方法求解时,它的 Galois 群的组合因数都是素数,即它的 Galois 群是可解群.

反之,如果一个方程在其系数域中的Galois群是可解群,则此方程必可用代数方法求解.

下面对这一点进行简单的说明. 先看一种特殊情况,即数域 **F** 上的方程:$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ 的次数 n 是素数的情况. 此时它的Galois群是由形如 $\alpha = (1\ 2\ 3\ \cdots n)$ 的置换所构成的循环群,$G = \{I, \alpha^2, \alpha^3 \cdots \alpha^{n-1}\}$,这个群是可解群,它的合成群列是 $G \supset I = \{(1)\}$.

设方程的根为 $x_1, x_2 \cdots x_n$,这 n 个根可用下面的方法求得.

设 ω 是 1 的 n 次原根. 考虑方程组

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n = r_0 = -a_1 \\ x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{n-1} x_n = r_1 \\ x_1 + \omega^2 x_2 + \omega^4 x_3 + \cdots + \omega^{2n-2} x_n = r_2 \\ \cdots\cdots \\ x_1 + \omega^{n-1} x_2 + \omega^{2n-2} x_3 + \cdots + \omega^{(n-1)^2} x_n = r_{n-1} \end{cases}$$

任取上述方程组中的一个方程

$$x_1 + \omega^k x_2 + \omega^{2k} x_3 + \cdots + \omega^{(n-1)k} x_n = r_k,$$

把置换 $\alpha = (1\ 2\ 3\ \cdots n)$ 作用于此方程的左边,得

$$x_2 + \omega^k x_3 + \omega^{2k} x_4 + \cdots + \omega^{(n-2)k} x_n + \omega^{(n-1)k} x_1,$$

这与用 ω^{-k} 乘方程的左边所得结果相同,这是因为 $\omega^n = 1$,故

$$\omega^{-k} = \omega^{nk} \cdot \omega^{-k} = \omega^{(n-1)k},$$

所以

$$x_2 + \omega^k x_3 + \omega^{2k} x_4 + \cdots + \omega^{(n-2)k} x_n + \omega^{(n-1)k} x_1 = r_k \omega^{-k},$$

因此置换 $\alpha = (1\ 2\ 3\ \cdots n)$ 把 r_k 变为 $r_k\omega^{-k}$,但$(r_k\omega^{-k})^n = (r_k)^n$,所以置换 α 不改变$(r_k)^n$ 的值,由于群 G 中的置换都是 α 的乘幂,所以 G 中的所有置换都不改变$(r_k)^n$ 的值. 由此 $(r_k)^n$ 必为 **F** 中的元素,可令$(r_k)^n = \alpha_k$,则$\alpha_k \in \mathbf{F}$,亦即 $r_k = \sqrt[n]{\alpha_k}$. 因此上面方程组可写成

$$\begin{cases} x_1 + x_2 + x_3 + \cdots + x_n = -a_1 \\ x_1 + \omega x_2 + \omega^2 x_3 + \cdots + \omega^{n-1} x_n = \sqrt[n]{\alpha_1} \\ x_1 + \omega^2 x_2 + \omega^4 x_3 + \cdots + \omega^{2n-2} x_n = \sqrt[n]{\alpha_2}. \\ \cdots\cdots \\ x_1 + \omega^{n-1} x_2 + \omega^{2n-2} x_3 + \cdots + \omega^{(n-1)^2} x_n = \sqrt[n]{\alpha_{n-1}} \end{cases}$$

其中 $\alpha_1, \alpha_2 \cdots \alpha_{n-1} \in \mathbf{F}$.

由于上面线性方程组，所以只要对

$$\omega,\ \omega^2,\ \cdots\ \omega^{(n-1)^2},\ \sqrt[n]{\alpha_1},\ \sqrt[n]{\alpha_2},\ \cdots\ \sqrt[n]{\alpha_{n-1}}$$

进行有限次加、乘、除运算，就可以解出 $x_1, x_2 \cdots x_n$，由此

$$x_1, x_2 \cdots x_n, \in F(\omega, \sqrt[n]{\alpha_1},\ \sqrt[n]{\alpha_2},\ \cdots\ \sqrt[n]{\alpha_{n-1}}),$$

即方程可用代数方法解出.

对于一般情况，若它在系数域中的 Galois 群是可解群，即合成群列 $G \supset G_1 \supset G_2 \supset \cdots G_s = I$，其中 G_i 是 G_{i-1} 的极大不变子群，且(G_{i-1} 的阶数)：(G_i 的阶数) $= r_i, i = 1, 2 \cdots s$　都是素数，则可以证明其根域 $\mathbf{N}$ 与系数域 $\mathbf{F}$ 之间也有相应的正规扩域序列

$$\mathbf{F} = \mathbf{K}_0 \subset \mathbf{K}_1 \subset \mathbf{K}_2 \subset \cdots \subset \mathbf{K}_s = \mathbf{N}, \text{且} [\mathbf{K}_i : \mathbf{K}_{i-1}] = r_i, i = 1, 2 \cdots s,$$

因为 $\mathbf{K}_{i+1}$ 是 $\mathbf{K}_i$ 的正规扩域，又 $\mathbf{K}_{i+1}$ 是 $\mathbf{K}_i (i = 0, 1, 2 \cdots s-1)$ 上某一方程 $p_i(x) = 0$ 的根域，可以证明 $p_i(x) = 0$ 在数域 $\mathbf{K}_i$ 中的 Galois 群是

$$\{I, \alpha = (1\ 2 \cdots r_{i-1}\ r_i),\ \alpha^2 \cdots \alpha^{r_i - 1}\}$$

上面简单地说明了方程能用根号求解(代数方法求解)的伽罗华条件的证明思路，由此可以看出其关键是正规扩域序列和相对不变自同构群的合成群列间的对应，而这也正是Galois 理论的核心内容. 这里只介绍了一些概念和直接引用了一些结论，至于这些结论的严格证明，限于篇幅，就不可能详细叙述了.

最后研究五次及五次以上方程不能用根号解出的问题；因 n 次代数方程的 Galois 群是对称群 $\mathbf{S}_n$，又当 $n > 4$ 时 $\mathbf{S}$ 不是可解群，所以 n 次代数方程当 $n > 4$ 时不能用根号解出，这就是下面的定理：

定理 6.5.3　五次及五次以上的代数方程不能用代数方法求解.

问题 6.5

1. 求证：当 $p > 7$ 时，$x^p - 1$ 素域 $\mathbf{Z}/(p)$ 上可用根号解.

2. 求证：$x^p - 1$ 素域 $\mathbf{Z}/(3)$ 上可用根号解.

3. 令 $x^3 + ax + b$ 在特征为 2 的域 F 上不可约，证明：它的 Galois 群或是 S_3 或是 A_3.

4. 令 $x^4 + ax^2 + b$ 在特征不为 2 的域 F 上不可约，G 是它的 Galois 群，证明：

(1) 若 b 是 F 中元素的平方，G 为 Klein 四元群；

(2) 若 b 不是 F 中元素的平方，但 $b(a^2 - 4b)$ 是，则 G 是 4 阶循环群；

(3) 若 b 与 $b(a^2 - 4b)$ 都不是 F 中元素的平方，则 G 是 8 阶群.

§6.6　尺规作图问题

本节我们讨论直尺与圆规作图问题. 什么是直尺与圆规作图问题呢？依照希腊人柏拉图的观点，最"完美的"几何图形就是直线和圆. 作一几何图形的工具只能是圆规与直尺(无刻度)，仅用这两种工具，哪些图形可以作出，这就是所谓的直尺与圆规作图问题.

用圆规和直尺可以作出许多图形，可以把一条线段分成任意多个相等的线段，可以把一个角二等分，可以画一条与已知直线平行的直线，以及作正三角形和正五边形等. 然而也有一些几何作图问题，仅用圆规与直尺这样的工具是不充分的. 两千多年前，古希腊人留给我们四个著名的几何作图难题，它们是：

(1) 化圆为方：

能否用圆规和直尺作出一正方形使其面积与给定圆的面积相等？

(2) 立方倍积：

给了任意一个正立方体，能否用圆规和直尺作出一个立方体，其体积是原立方体体积的 2 倍？

(3) 三等分任意角：

能否用圆规和直尺三等分任意角？

(4) 分圆问题：

对于 $\forall\, n \geqslant 3$，能否用圆规和直尺作出一个正 n 边形？

毫不奇怪，古希腊人发现解决以上这四个问题是特别困难的，他们用圆规和直尺无法作出这些图形. 但是他们也不能证明这些图形不能作出，因而他们花费了大量的聪明才智去探寻这些问题的解答，特别是阿基米德使用极限的技巧取得了 $3\,\frac{10}{71} < \pi < 3\,\frac{1}{7}$ 这样惊人的成就，但是仍然无助于问题的解决.

这些问题在历史上曾经困扰古人很长时期，直到出现近世代数，这些问题直到 19 世纪才被证明是不可能问题. 我们通过笛卡尔的划时代的工作 —— 引入坐标系，把代数和几何联系起来，它使我们能把几何问题转化为代数问题，这样我们再借助于域扩张和 Galois 理论可以给出上述 4 个问题一个圆满的回答，因而也是用代数方法解决几何

问题的典范. 但是,由于中学里不可能学习近世代数,因而不断有一些只具中学数学知识的青年还在研究这些问题,应该劝导他们不要再在这些问题上浪费时间. 下面来看近世代数是如何解决这些问题的. 首先,我们要把这些问题化为近世代数的问题.

为了阐述尺规作图的可能性的充要条件,我们首先需把几何问题转换成代数语言. 为此,还需把尺规作图的准则再强调一下.

1. 几何作图问题的代数提法

设在平面上已知 m 个点,我们选择直角坐标系和确定点(0,1),并设在此坐标系中已知的 m 个点的坐标为 $(x_1,y_1),\cdots,(x_m,y_m)$,令 $\mathbf{F}=Q(x_1,y_1,\cdots,x_m,y_m)$,从这些已知点出发通过有限次下列操作可构造出的点称为**可构造点**,对应的坐标称为**可构造数**. 这些操作是:

(1) 过已得到的两点画一条直线;

(2) 以某个点为圆心,以某两个点之间的距离为半径画圆;

(3) 计算并标出两直线的交点坐标;

(4) 计算并标出一直线和一圆的交点坐标;

(5) 计算并标出两圆的交点坐标.

因而尺规作图问题化为求出所有可构造数的问题.

一个平面几何作图问题就是从已知的有限个图形(点、直线、圆等),用圆规和直尺作出适合已知条件的几何图形. 一个几何图形可作出就是利用我们的假设作出一些适当的点、线和圆. 但直线和圆都可由点来决定,故用圆规和直尺作图问题可以看为由已知点作出适合某些条件的点的问题. 又借助于坐标系,作点的问题可看为作复数的问题. 因而我们讨论的圆规与直尺作图问题就是从有限个复数出发,得到所要的复数. 这样作图问题完全转化为代数问题. 为此我们引进下列概念.

设 F 是域,域 E 称为 F 的平方根域,若 $E=F(\alpha)$,其中 $\alpha^2\in F$,记 $\alpha=\sqrt{a_i}$,其中 $a\in F$,一个域扩张链

$$F=F_0\subseteq F_1\subseteq F_2\subseteq\cdots\subseteq F_k\subset\mathbf{C}$$

称为平方根域链,若对每个 i,F_i 是 F_{i-1} 的平方根域.

2. 可构造数基本定理

定理 6.6.1　设 $\mathbf{K}$ 是所有可构造数的集合,则 $\mathbf{K}$ 是实数域 $\mathbf{R}$ 的子域,是有理数域 $\mathbf{Q}$ 的扩域,即 $\mathbf{Q}\leqslant\mathbf{K}\leqslant\mathbf{R}$.

证明　首先证 $\mathbf{K}$ 是一个数域,对任何 $a,b\in\mathbf{K}$,$a+b$ 可用圆规、直尺做出(以下简

称"可做出")，故 $a+b\in\mathbf{K}$，ab 可做出(见图 6.5)，故 $ab\in\mathbf{K}$，对 $\forall\ a\in\mathbf{K}, a\neq 0, a^{-i}$ 可做出，故 $a^{-i}\in\mathbf{K}$，所以 $\mathbf{K}$ 是一个域. 再证 $\mathbf{K}$ 是 $\mathbf{Q}$ 的扩域：由于已知(0,1)，故 $Q=\{\frac{m}{n}\Big| m, n\in\mathbf{Z}, n\neq 0\}$ 中元素均可做出，所以 $\mathbf{Q}\subseteq\mathbf{K}$. 最后证 $\mathbf{K}$ 是 $\mathbf{R}$ 的子域，因直线与圆的交点坐标和圆之间的交点坐标除涉及 $+$，$-$，$\times$，$\div$ 运算外，只涉及正数的开平方运算，而正数 a 开平方可做出(见图 6.5)，且 $\sqrt{a}\in\mathbf{R}$，所以 $\mathbf{K}\subseteq\mathbf{R}$.

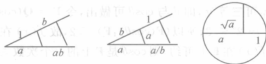


图 6.5

定理 6.6.2(可构造数的充要条件)　实数 α 可构造的充分必要条件是存在一个有限的域链：

$$\mathbf{F}=\mathbf{K}_0\leqslant\mathbf{K}_1\leqslant\mathbf{K}_2\leqslant\cdots\leqslant\mathbf{K}_n\leqslant\mathbf{R},$$

满足 $(\mathbf{K}_{i+1}:\mathbf{K}_i)=2(i=0,1,\cdots,i-1)$ 和使 $\alpha\in\mathbf{K}_n$.

证明　先证充分性. 设有以上域链使 $\alpha\in\mathbf{K}_n$，因已知点(0,1)，对 1 作四则运算可得 Q 中任何元素，故 Q 中元素均可做出，类似可证 $\mathbf{F}=Q(x_1, y_1, \cdots, x_m, y_m)$ 中任何数均可做出，现设 $\mathbf{K}_{i-1}$ 可做出(指 $\mathbf{K}_{i-1}$ 中任何元素可做出).

因为 $(\mathbf{K}_i:\mathbf{K}_{i-1})=2$，可设 $\mathbf{K}_i$ 在 $\mathbf{K}_{i-1}$ 上的线性空间的基为 $1,\theta$，则 $1,\theta,\theta^2$ 线性相关，存在 $a,b\in\mathbf{K}_{i-1}$ 使 $a\theta^2+b\theta+c=0(a\neq 0)$，得

$$\theta=(-b\pm\sqrt{b^2-4ac})/(2a),$$

知 θ 可做出，且 $\mathbf{K}_i=\mathbf{K}_{i-1}(\theta)=\{k_1+k_2\theta\,|\,k_1,k_2\in\mathbf{K}_{i-1}\}$，所以 $\mathbf{K}_i$ 中任意元素均可做出. 以此类推可得，$\mathbf{K}_n$ 中任何元素均可做出，因而 α 可做出.

再证必要性：设 α 可构造，则在 $\mathbf{F}$ 上通过有限步操作(i)～(v)可得到 α，设在这有限步操作中逐次作出数 $a_1, a_2, \cdots, a_m=\alpha$. 并令

$$\mathbf{K}_i=\mathbf{K}_{i-1}(\alpha_i)(i=1,2,\cdots,m).$$

由于每次操作是对已知可构造数进行四则运算或开方，故 $(\mathbf{K}_i:\mathbf{K}_{i-1})=1$ 或 2. 由此可得如上之域链.

推论 6.6.3(可构造数的必要条件)　若 $\alpha\in\mathbf{R}$ 可构造，则 $(\mathbf{F}(\alpha):\mathbf{F})=2^n$，$n$ 为非负整数.

3. 若干几何作图问题的解

根据以上定理，立即可以推出，两倍立方体问题与圆化方问题都是不可能用圆规直

尺解决的. 对于三等分任意角问题有以下定理：

定理 6.6.4　角 φ 可以三等分的充分必要条件是多项式 $4x^3-3x-\cos\varphi$ 在 $\mathbf{Q}(\cos\varphi)$ 上可约.

证明　首先,由已知 φ 可做出 $\cos\varphi$. 设 $\varphi=\theta/3$,由公式

$$\cos\varphi=\cos3\theta=4\cos^3\theta-3\cos\theta$$

可得 $\cos\theta$ 是多项式 $f(x)=4x^3-3x-\cos\varphi$ 的根.

先证必要性:设 φ 可三等分,即 θ 与 $\cos\theta$ 可做出,令 $\mathbf{F}=\mathbf{Q}(\cos\varphi)$,由定理 6.6.6 的推论得,$(\mathbf{F}(\cos\theta):\mathbf{F})=2^n\leqslant3$,所以$(\mathbf{F}(\cos\theta):\mathbf{F})\leqslant2$,故 $f(x)$ 在 $\mathbf{F}$ 上可约.

再证充分性:若 $f(x)$ 在 $\mathbf{F}$ 上可约,则 $\cos\theta$ 是 $\mathbf{F}$ 上的一个次数 $\leqslant2$ 的多项式的根,故有$(\mathbf{F}(\cos\theta):\mathbf{F})\leqslant2$,由定理 6.6.3,$\cos\theta$ 可做出.

关于分圆问题讨论如下:首先,由 $\pi/3$ 不能三等分可得出正 18 边形不能做出,因而不能将圆周任意 n 等分. 我们先证以下结果.

定理 6.6.5　设 p 是素数,若正 p 边形可做出,则 p 是如下形式的费尔马素数:$p=2^m+1$,m 为不小于零的整数.

证明　设 $\xi=\cos\dfrac{2\pi}{p}+\mathrm{i}\sin\dfrac{2\pi}{p}$,若正 p 边形可做出,即 $\cos\dfrac{2\pi}{p}$,$\sin\dfrac{2\pi}{p}$ 可做出,由上推论得出,

$$\left[\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p}\right):\mathbf{Q}\right]=2^k,\left[\mathbf{Q}\left(\cos\frac{2\pi}{p},\ \sin\frac{2\pi}{p},\ \mathrm{i}\right):\mathbf{Q}\right]=2^{k+1},$$

而 $\mathbf{Q}(\xi)\subseteq\mathbf{Q}\left(\cos\dfrac{2\pi}{p},\ \sin\dfrac{2\pi}{p},\mathrm{i}\right)$,所以$[\mathbf{Q}(\xi):\mathbf{Q}]=2^r,r\leqslant k+1$.

另一方面,ξ 是多项式 $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 的根,$f(x)$ 在 $\mathbf{Q}$ 上不可约,故有$[\mathbf{Q}(\xi):\mathbf{Q}]=p-1$. 由此得 $p-1=2^r$,$p=2^r+1$. 由于 p 为素数,r 必须是 2 的幂,所以 $p=2^{2^m}+1$.

由定理 6.6.3 可以得到三等分任意角问题否定的回答,只举反例即可.

例 6.6.1　三等分任意角.

取 $\varphi=\pi/3$,则 $\mathbf{F}=\mathbf{Q}(\cos\varphi)=\mathbf{Q}$,多项式 $f(x)=4x^3-3x-\cos\varphi=4x^3-3x-1/2$,在 $\mathbf{Q}$ 上不可约(见"高等代数"内容),所以 φ 不能三等分.

例 6.6.2　化圆为方.

不妨取圆的半径为 1,那么圆的面积为 π,将它化为等面积的正方形,就是要求满足 $x^2=\pi$ 的正方形边长 x,但 π 是超越数(不存在有理系数多项式以 π 为根),故 x 对于 $\mathbf{Q}$ 亦为超越元,它不可能从 $\mathbf{Q}$ 出发用尺规作出.

例 6.6.3　立方倍积.

不妨取立方体的一边长为 1,作出体积是它 2 倍的立方体即是要求满足 $x^3=2$ 的复

数 x. 但 x 在 $\mathbf{Q}$ 上的次数为 3，不是 2 的幂，故不能用尺规作出.

例 6.6.4 正 $n(\geqslant 3)$ 边形作图问题.

ζ 可用尺规作出 $\Leftrightarrow$ ζ 的次数 $\varphi(n)$ 应为 2 的方幂，从而推出 $e_1 = e_2 = \cdots\cdots = e_r = 1$，而 $p_i - 1 = 2^{k_i}$，我们把 $p_i = 2^{k_i} + 1$ 称为费尔马素数. 因此，只有当 n 能分解成 2 的方幂与有限个费尔马素数的积时，正 n 边形才能用尺规作出. 已知的费尔马素数有 3，5，17，257 和 65537.

首先，由 $\pi/3$ 不能三等分可得出正 18 边形不能做出，因而不能将圆周任意 n 等分. 我们在这里只讨论素数边形的作图问题.

设 p 是一个素数. 显然一个正 p 边形的作图问题等价于要作出点 $z = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$ z 适合多项式 $x^p - 1 = 0$，而 $x^p - 1 = (x-1)(x^p + x^{p-1} + x^{p-2} + \cdots + 1)$，于是 z 适合一个 $p-1$ 次多项式 $x^p + x^{p-1} + x^{p-2} + \cdots + 1$.

由 Eisenstein 判别法不难证明这是 Q 上的一个不可约多项式，即是 z 的极小多项式.

若这个正 p 边形可用尺规作出，则 $p - 1 = 2^m$，或 $p = 2^m + 1$.

从这个结论我们立即可推出正七边形、正十一边形等均不能用直尺与圆规作出，因为这些素数都不能写成 $2^m + 1$ 的形式，我们还可以进行更深入一些的讨论，设上述 m 含有一个奇数因子，比如 $m = kq$，其中 q 是奇数，则

$$2^m + 1 = 2^{kq} + 1 = (2^k)^q + 1 = (2^k + 1),$$

即这时，$2^m + 1$ 是一个合数. 因此要使 $2^m + 1$ 是素数，m 必须具有形状 2^t. 形如 $2^{2^5} + 1$ 的素数称为 Fermat 数. Fermat 曾猜测形如 $2^{2^t} + 1$ 的数都是素数，Euler 指出这个猜测不成立，因为 $2^{2^5} + 1$ 是一个合数. 当 $t = 0,1,2,3,4$ 时，$2^{2^t} + 1$ 确实都是素数，它们依次为

$$3,5,17,257,65537,$$

这是迄今为止人们所知的全部 Fermat 数. 有人猜测这是仅有的五个 Fermat 数，但至今未能证实，也未能否定.

现在我们得到了一个正 p 边形可用圆规、直尺作出的必要条件是：p 是一个 Fermat 素数.

Gauss 定理 正 n 边形可用尺规作出的充分必要条件是 $n = 2^r p_1 p_2 \cdots p_t$，其中 $r \geqslant 0$，p_i 为互不相同的 Fermat 数.

对已知的五个 Fermat 数，正多边形的作图都已有人具体地构造出来. 比如正十七边形的作法是 Gauss 19 岁时的惊人之作，而正 257 边形及正 65537 边形虽然已有人作出，但因无什么重要价值而只配放进博物馆供人欣赏.

例 6.6.5　下面我们给出正十七边形的作法.

令 $\theta = 2\pi/17, \varepsilon_k = \cos k\theta + i\sin k\theta$,则 $\varepsilon_1, \cdots, \varepsilon_{16}$ 是方程 $\frac{x^{17}-1}{x-1} = x^{16} + \cdots + x + 1$ 的零点.

下面我们用初等技巧证明 $\cos\theta$ 可由根式表出,从而正 17 边形可由直尺与圆规作出.

因为 3 为模 17 的原根,我们有

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^m(\mathrm{mod}17)$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

定义

$$x_1 = \varepsilon_1 + \varepsilon_9 + \varepsilon_{13} + \varepsilon_{15} + \varepsilon_{16} + \varepsilon_8 + \varepsilon_4 + \varepsilon_2;$$
$$x_2 = \varepsilon_3 + \varepsilon_{10} + \varepsilon_5 + \varepsilon_{11} + \varepsilon_{14} + \varepsilon_7 + \varepsilon_{12} + \varepsilon_6.$$
$$y_1 = \varepsilon_1 + \varepsilon_{13} + \varepsilon_{16} + \varepsilon_4;$$
$$y_2 = \varepsilon_9 + \varepsilon_{15} + \varepsilon_8 + \varepsilon_2;$$
$$y_3 = \varepsilon_3 + \varepsilon_5 + \varepsilon_{14} + + \varepsilon_{12};$$
$$y_4 = \varepsilon_{10} + \varepsilon_{11} + \varepsilon_7 + \varepsilon_6.$$

我们有

$$\varepsilon_k + \varepsilon_{17-k} = 2\cos k\theta, k = 1,2\cdots 16$$

从而又有

$$x_1 = 2(\cos\theta + \cos 8\theta + \cos 4\theta + \cos 2\theta);$$
$$x_2 = 2(\cos 3\theta + \cos 7\theta + \cos 5\theta + \cos 6\theta).$$
$$y_1 = 2(\cos\theta + \cos 4\theta);$$
$$y_2 = 2(\cos 8\theta + \cos 2\theta);$$
$$y_3 = 2(\cos 3\theta + \cos 5\theta);$$
$$y_4 = 2(\cos 7\theta + \cos 6\theta).$$

又 $x_1 + x_2 = -1$,另一方面,利用上面二式及三角恒等式

$$2\cos m\theta\cos n\theta = \cos(m+n)\theta + \cos(m-n)\theta,$$

又有 $x_1 x_2 = -4$,因而 x_1 和 x_2 都是多项式 $x^2 + x - 4$ 的零点,且 $x_1 > 0, x_1 > x_2$,类似地 $y_1 + y_2 = x_1, y_1 y_2 = -1$,因而 y_1 和 y_2 又是多项式 $x^2 - x_1 x - 1$ 的零点,且 $y_1 > y_2$,同理 y_3 和 y_4 又是多项式 $x^2 - x_2 x - 1$ 的零点,且 $y_3 > y_4$. 现在我们有

$$2\cos\theta + \cos 4\theta = y_1, 4\cos\theta\cos 4\theta = 2(\cos 5\theta + \cos 3\theta) = y_3.$$

可以验证 $2\cos\theta, 2\cos 4\theta$ 是多项式 $x^2 - y_1 x + y_3$ 的零点,且 $\cos\theta > \cos 4\theta$.

解方程

$$x^2+x-4,\ x^2-x_1x-1,\ x^2-x_2x-1,\ x^2-y_1x+y_3,$$

得

$$\cos\theta = 1/16\ \sqrt{17}-1+\sqrt{34-2\sqrt{17}}$$
$$+2\sqrt{17+3\sqrt{17}+\sqrt{170-26\sqrt{17}}-4\sqrt{34+2\sqrt{17}}}$$

最后利用 Galois 理论给出著名的代数基本定理的另一个证明.

引理 6.6.6 $\mathbf{R}[x]$ 的每个奇数次多项式 $f(x)$ 必有实根，进一步地，$\mathbf{R}$ 没有大于 1 的奇数次扩张.

证明 设 $f(x)=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n\in\mathbf{R}[x]$，

令 $t=1+\sum|a_i|$，于是对所有的 i，$|a_i|\leqslant t-1$，令 $h(x)=f(x)-x^n$，则

$$|h(t)|=|a_0+a_1t+\cdots+a_{n-1}t^{n-1}+a_nt^n|$$
$$\leqslant(t-1)(1+t+\cdots+t^{n-1})=t^n-1<t^n,$$

故 $-t^n<h(t)$，因而 $f(t)=h(t)+t^n>0$.

另一方面，类似地可得 $|h(-t)|<t^n$，于是又有 $f(-t)=h(-t)+(-t)^n<t^n+(-t)^n$.

当 n 为奇数时，就是 $f(-t)<0$，由连续函数的介值定理知，存在一个实数 r 使得 $f(r)=0$，即 $f(x)$ 有一个实根.

设 E 是 $\mathbf{R}$ 的有限扩域，对于 $\delta\in E$，设 δ 在 $\mathbf{R}$ 上的极小多项式为 $p(x)$，由推论 4.5.5 知

$$[\mathbf{R}(\delta):\mathbf{R}]=\deg p(x),$$

由上述证明可得 $\deg p(x)$ 必为偶数.

代数基本定理 复数域 $\mathbf{C}$ 上每个 $n(\geqslant 1)$ 次多项式有 n 个复数根.

证明 设 $f(x)=\sum a_ix^i\in\mathbf{C}[x]$，只证 $f(x)$ 在 $\mathbf{C}$ 内有一个根即可. 令 $\overline{f(x)}=\sum\overline{a_i}x^i$，其中 $\overline{a_i}$ 是 a_i 的共轭数，设 $f(x)\overline{f(x)}=\sum c_kx^k$，其中 $c_k=\sum_{i+j=k}a_i\overline{a_j}$，从而 $\overline{c_k}=c_k$，故 $f(x)\overline{f(x)}\in\mathbf{R}[x]$. 若 $f(x)$ 有一个复根 ω，则 ω 是 $f(x)\overline{f(x)}$ 的一个根.

反之，若 ω 是 $f(x)\overline{f(x)}$ 的一个根，则 ω 是 $f(x)$ 的根，或是 $\overline{f(x)}$ 的根，但若 ω 是 $\overline{f(x)}$ 的根，则 $\overline{\omega}$ 是 $f(x)$ 的根，由此可得 $f(x)$ 有一个复根当且仅当 $f(x)\overline{f(x)}$ 有一个复根. 因而只需证每个实系数多项式有一个复根即可.

设 $p(x)\in\mathbf{R}[x]$ 是次数 >1 的不可约多项式，E 是 $\mathbf{R}$ 的包含 $\mathbf{C}$ 的 $(x^2+1)p(x)$ 的分裂域，因为 $\mathrm{char}\mathbf{R}=0$，故 $E/\mathbf{R}$ 是 Galois 扩张. 令 G 是其 Galois 群 $|G|=2^mk$，其中 $m\geqslant 0$，2 不整除 k，由第二章的 Sylow 定理，G 有 2^m 阶的子群 H，令 $K=E^H$ 是与 H 对应

的中间域，则 $R\subseteq K\subseteq E$，从而$[K:\mathbf{R}]=[G:H]=k$，得 $k=1$，故 $|C|=2^m$.

因为 $i\in\mathbf{C}$，于是$[\mathbf{C}:\mathbf{R}]=2$，又$[E:\mathbf{R}]=[E:\mathbf{C}][\mathbf{C}:\mathbf{R}]$，由此得$[E:\mathbf{C}]=2^{m-1}$. 若 $m-1\geqslant 1$，则 $G(E/\mathbf{C})$ 有 2^{m-2} 阶正规子群 N，由 Galois 理论的基本定理

$$[E:E^N]=|N|,且[E^N:\mathbf{C}]=[E:\mathbf{C}]/[E:E^N]=2,$$

于是E^N是$\mathbf{C}$上2次扩张. 因为$i\in\mathbf{C}$，故由二次方程的求根公式可知，$\mathbf{C}$上二次多项式均为可约多项式，这是一个矛盾，故 $m-1=0$，从而 $E=\mathbf{C}$.

拉格朗日小传

拉格朗日(J. L. Lagrange)，1736 年 1 月 25 日出生在意大利，祖先是法国人. 早年他阅读一篇由英国天文学家哈雷(E. Halley，1656—1742) 写的关于牛顿微积分的论文时就深深地被数学所吸引. 19 岁时，他成了都灵皇家炮兵学校的数学教授. 拉格朗日对数学和物理的许多领域有过重要的贡献，这些领域包括数论、方程论、常微分方程和偏微分方程、变分学、解析几何、流体力学以及天体力学.

Lagrange 关于用根式求解一元三次和四次代数方程的方法为 Galois 用群论方法解多项式的理论(即 Galois 理论) 的建立打下了扎实的基础. Lagrange 还是一位很好的作家，他的文笔流畅、风格清新. 40 岁时，Lagrange 被任命为柏林科学院的院长，以接替欧拉. 1787 年，他应路易十六的邀请访问巴黎，成为国王和王后的好朋友.

1793 年，Lagrange 领导了一个其成员包括拉普拉斯和法国化学家拉瓦锡(A. L. Lavoisier，1743—1794) 在内的委员会，致力于设计一种新的重量和长度系统，其结果是米制的诞生. 他曾先后 5 次获得法兰西科学院奖金.

Lagrange 于 1813 年 4 月 10 日在巴黎逝世.

问题 6.6

1. 求下列扩张的 Galois 群 G：

(1)$Z/<p>(\omega)$ 关于 $Z/<p>$ 的 Galois 群；

(2)$Q(\omega)$ 关于 Q 的 Galois 群. (这里 $\omega^2+\omega+1=0$)

2. 令 $E=C(x)$，C 为复数域，$\omega^2+\omega+1=0$，令自同构 $\tau:x\to x^{-1}$，$\sigma:x\to\omega x$. 求证：(1)$\sigma^2=e$，$\tau^2=e$，$\sigma\tau=\tau^{-1}\sigma$；

(2) 求出 σ，τ 生成的子群 H.

3. 求证：域 F 上的 3 次不可约多项式的分裂域 E 关于 F 的 Galois 群或是对称群或是交代群.

4. 设 $p_1,p_2\cdots p_r$ 是 r 个不同的素数，试求 E关于 Q 的 Galois 群，这里 $E=Q(\sqrt{p_1}$，

$\sqrt{p_2} \cdots \sqrt{p_r})$.

5. 令 $E = \mathbf{Q}(\mathrm{i}, \sqrt[4]{2})$，求 E 关于 $\mathbf{Q}$ 的 Galois 群，并求其子群所对应的子域.

6. 试决定 $x^4 - 2$ 在 $\mathbf{Q}$ 上的分裂域的所有子域及相应的 Galois 群 G 的子群.

7. 设 E 是域 F 的可离正规扩张，G 为 Galois 群，设 L 是 E、F 的中间域，H 为 E 关于 L 的 Galois 群，令 $N = \{\sigma \in G \mid \sigma(L) = L\}$，证明：

(1)　N 是 H 在 G 中的正规化子；

(2)　L 关于 F 的 Galois 群 $G_{L/F} \cong N/H$.

8. (1) 设 E 为 $\mathbf{Q}$ 的 2 次扩张，求 $x^3 - 3x + 1$ 在 E 上的 Galois 群；

(2) 求 $x^4 - 2$ 在 $\mathbf{Q}(\mathrm{i})$ 上的 Galois 群.

9. 如果域 F 含有 n 次本原单位根，且 E 为 $f(x) = (x^n - a_1)(x^n - a_2)\cdots(x^n - a_n)$ $a_i \in F$，在 F 上的分裂域，那么 E 是 F 的 Abel 扩张，且 Galois 群 G 中之任意元素的周期必为 n 的因数.

10. 设 $f(x) \in \mathbf{Q}(x)$ 是一个 $n(n > 4)$ 次不可约多项式且 $f(x)$ 在 $\mathbf{Q}$ 上的 Galois 群 $G \cong S_n$，设 E 是 $f(x)$ 在 $\mathbf{Q}$ 上的分裂域，$\alpha \in E$ 为 $f(x)$ 的一根，证明：$(\mathbf{Q}(\alpha):\mathbf{Q}) = n$，但 $\mathbf{Q}(\alpha)$ 关于 $\mathbf{Q}$ 的 Galois 群 H 为单位元群.

11. 令 F 是实数域的子域，$f(x)$ 是 F 上不可约 4 次多项式. 令 G 为 f 的 Galois 群，如果 f 恰有两个实根，那么 G 是 S_4 或是阶为 8 的子群.

12. 设域 F 中含有全部的 n 次单位根，n 是与 $\mathrm{char}F$ 互素的一个正整数，并且对 n 的任意因数 $r > 1$，a 与 b 在 F 中均无 r 次方根. 如果 E 是 $(x^n - a)(x^n - b)$ 在 F 上的分裂域，那么 $F(\sqrt{a}) = F(\sqrt{b}) \Leftrightarrow a = b^m c^m, c \in F(m, n) = 1$.

13. 试给出正五边形的作图步骤.

14. 能否用尺规三等分 45°，75°，90° 角？

第 7 章 Lie 群的结构与对称性

Lie 群是群论中极其重要的部分，Lie 群是代数结构和几何结构的自然结合体，它有相当完美的对称性. Lie 群的结构丰富，而且具有深刻的内在理论. 在很多领域，例如研究数学中的特殊函数、处理生物光学中的视觉问题、研究一般有序介质材料、液晶材料、超弹性材料以及许多工程领域都有广泛的应用.

Lie 群及相应的 Lie 代数早期主要应用于原子和原子核的壳层结构，而后在基本粒子物理学中得到最广泛的应用. 现代粒子物理的基本框架就是由 Lie 群给出的. 夸克模型的基本对称性可以由 $SU(3)$、$SU(4)$ 或 $SU(6)$ 给出. 各种大统一模型则有 $SU(5)$、$SU(10)$、$E(6)$ 等理论. 总之，离开 Lie 群，现代粒子物理论就无从谈起.

Lie 群是特殊的连续群，本章主要研究 Lie 群的对称性质.

§7.1 群代数和群流形

定义 7.1.1 如果对于群 G 的每一个元素，均有一个确定的数 $f(g_i)$ 与之对应，即 $\forall\ g_i \in G$，有映射 $f: g_i \to f(g_i)$，$\forall\ g_i \in \mathbf{C}$(复数域)，则称集合 $\{f(g_i)\}$ 为群函数，亦可记为 $f(G)$.

对于有限群，群函数可取平均值，$\overline{f(G)} = \dfrac{1}{n}\sum\limits_{g_i \in G} f(g_i)$ (n 为群 G 的阶). 显然，若 $f(g_i) \geqslant 0$，($\forall\ g_i \in G$)，则 $\overline{f(g_i)} \geqslant 0$，并具有线性性质：

$$\overline{af_1(G) + bf_2(G)} = a\,\overline{f_1(G)} + b\,\overline{f_2(G)}.$$

由重排定理，若 $g_j \in G$，

$$\overline{f(G)} = \frac{1}{n}\sum_{g_i \in G} f(g_i) = \frac{1}{n}\sum_{g_i \in G} f(g_i g_j) = \frac{1}{n}\sum_{g_i \in G} f(g_j g_i) = \frac{1}{n}\sum_{g_i \in G} f(g_i^{-1}).$$

定义 7.1.2 以群元 g_i 作为基，其所有线性组合构成 n 维线性空间 L_n，其中任意矢量 $X = \sum\limits_{g_i \in G} f(g_i) g_i$，$Y = \sum\limits_{g_i \in G} \varphi(g_i) g_i$，$f(g_i)$ 和 $\varphi(g_i)$ 为群 G 的群函数，在 L_n 中定义加法满足通常线性空间的矢量加法规则：

$$c_1X + c_2Y = \sum_{g_i \in G}(c_1 f(g_i) + c_2\varphi(g_i))g_i.$$

再定义 L_n 中数乘运算(内积)：

$$XY \equiv (\sum_{g_i \in G} f(g_i)g_i)(\sum_{g_i \in G}\varphi(g_k)g_k)$$
$$= \sum_{g_i, g_k \in G} f(g_i g_k^{-1}) g_i g_k^{-1} \varphi(g_k) g_k$$
$$= \sum_{g_i, g_k \in G} f(g_i g_k^{-1}) \varphi(g_k) g_i \in L_n,$$

则 L_n 是封闭的，构成代数.

数论实际上包含代数、流行和拓扑学的概念. 我们在此简述以后要用到的拓扑和流形最基本的概念.

定义 7.1.3　设有开集合 $\{A_i\}$ 的一个族 B，其中脚标为 1，2，3 …，也可以是连续变化的. 如果对任何有限次并集，有 $\bigcup A_i \in B$，且对任何有限次相交，有 $A = \bigcap A_i \in B$，则称并集为构成拓扑空间 (A, A).

例 7.1.1　n 维欧氏空间 E_n. 令 $A_i \equiv S(a_i, r)$，x 为 E_n 中任意点的位置矢量，a_i 为某点的位置矢量；令 $|x - a_i| < r$，即在以 a_i 为球心、r 为半径的球内(不包含球面)，显然 $S(a_i, r)$ 为开集，则

$$A \equiv \bigcup_{a_i} S(a_i, r) \in E_n; \ \bigcap^{a_i} S(a_i, r) \in E_n.$$

因 (A, E_n) 构成拓扑空间，A 则为 E_n 的一个拓扑.

定义 7.1.4　如果开集 A_i 的数目有限，则称 $X = \bigcup A_i$ 为紧致空间.

例 7.1.2　E_n 内任何有界区域 $\triangle E_n$，它总可用有限个开集 $S(a_i, r)$ 的并集所覆盖.

例 7.1.3　任何有限个集合构成的并集是紧致的.

例 7.1.4　一维平移群 T_1. 令 $T(a_i)$ 代表直线上到原点距离为 a_i 的一个点，则 $T(a_i)$ 在直线各点连续跑动所得到的集合表示一条无限长直线或 E_1(图 7.1).

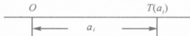


图 7.1

显然，T_1 是非紧致的，而其任何有限部分为紧致的. T_1 就是群流形的实例.

定义 7.1.5　称群流形的体积为群体积.

例 7.1.5　令 T_1 群的群元 $g_i = T(a_i)$，定义相应群流形体积元为

$$d\mu(g_i) = da_i,$$

则对于固定群元素 $g_i = T(a_i)$，体积元是不变的(图 7.2). 事实上，

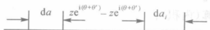


图 7.2

$$d\mu(g_ig_j) = d\mu(g_jg_i) = d\mu(g_i) = da_i \equiv da.$$

整个群 T_1 的体积

$$V = \int_{-\infty}^{\infty} d\mu(g_i) = \int_{-\infty}^{\infty} da \to \infty.$$

如果群流形是封闭和有界的，则群是紧致的，否则为不紧致的. 由此可知 T_1 为不紧致的. 这样，我们从另一个角度又得到例 7.1.4 的结论.

例 7.1.6 相角因子群 $U(1)$.

其定义是，群元 $U(\theta): z \xrightarrow{U(\theta)} z' = ze^{i\theta}$，其中 $z \in \Omega(C), \theta \in \Omega(R)$(实数域). 因此 $U(1) = \{U(\theta) \mid 0 \leqslant \theta \leqslant 2\pi\}$.

$$U(\theta)U(\theta'): U(\theta)U(\theta')z = U(\theta)(ze^{i\theta'}) = ze^{i\theta} \cdot e^{i\theta'}$$
$$= ze^{i(\theta+\theta')} = ze^{i(\theta'+\theta)} = U(\theta')U(\theta)z,$$

即 $U(1)$ 为 Abel 群，

$$U(\theta')U(\theta) = U(\theta+\theta') = U(\theta'+\theta).$$

与群 T_1 不同的是，

$$U(\theta + 2\pi) = U(\theta).$$

下面给出 $U(1)$ 群的流形. 令 $U(\theta_i)$ 表示单位圆上一个点，如图 7.3 所示，随着群参数 θ_i 在定义域从 0 到 2π 变化，代表点画出 $U(1)$ 群的群流形，即是单位圆. 其体积有限，流形有界，故此群为紧致群. 作群积分验证之：

令 $g_i = U(\theta_i)$，$d\mu(g_i) = d\theta_i$，显然，

$$d\mu(g_i) = d\mu(g_jg_i) = d\mu(g_ig_j) = d(\theta_i) \equiv d(\theta) = \text{cosst}$$

故群体积

$$V = \int_{U(1)} d\mu(g_i) = \int_0^{2\pi} d\theta = 2\pi.$$

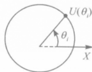


图 7.3

可知 T_1 为不紧致的. 这样，我们从另一个角度又得到例 7.1.4 的结论.

例 7.1.7 三维旋转群 R_3[以后记为 $O(3,R)$].

$\forall\, g_i \in R_3$，群元 g_i 可用单位矢量 n^0 与绕 n 的自转 $\Psi(0 \leqslant \Psi \leqslant \pi)$ 表示. 取半径为 π 的球体，令球内一点 P 表示转动 $g_i(n, \Psi)$，其中 n 是 $\overline{OP}$ 的方向，

$|\overrightarrow{OP}| = \Psi$,则群流形即为此球(图 7.4 不包括球面). 显然流形是有界的,故 R_3 也是紧致的.

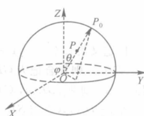


图 7.4　R_3 的流形

将 n 用球坐标表示 $n = n(\sin\theta, \cos\varphi\Psi, \sin\theta\sin\Psi, \cos\theta)$,则 $g = g(\Psi,\theta,\varphi)$,不变体积元为 $\mathrm{d}\mu(g) = \Psi^2\mathrm{d}\Psi\sin\theta\mathrm{d}\theta\mathrm{d}\varphi$,群流形体积

$$V = \int \mathrm{d}\mu(g) = \int_0^{2\pi}\mathrm{d}\Psi \cdot \Psi^2\int_0^{\pi}\sin\theta\mathrm{d}\theta\int_0^{2\pi}\mathrm{d}\varphi = \frac{3}{4}\pi^3 < \infty.$$

至于为何 Ψ 只取到 π 的原因是在 $\Psi = \pi$ 时,绕 n 转动 π,与绕 $-n$ 转动 $-\pi$ 实际上是相同的. 因此在球面上直径两端点 P 与 P' 系表示相同转动. 由此出现 O_3 在拓扑上有双连通结构,从而导致双值旋量表示等等问题的出现. 这反映物理上同一个转动,可以在右手系中实现,亦可在左手系中实现. $O(3, R)$ 只取右手系,故 $0 \leqslant \Psi \leqslant \pi$,因为在 $\pi \leqslant \Psi \leqslant 2\pi$ 所表示是相同转动,可通过反向转动得到.

例 7.1.8　　幺正群 $U(n)$.

$U(n)$ 的群元为 $n \times n$ 幺正矩阵,即

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \cdots & \cdots & & \cdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix},$$

其中 $\forall\ A_{ij}(n \leqslant i, j \leqslant n) \in \Omega(C)$,为 n^2 个复参数,群流形为 n^2 维酉空间. 幺正条件为 $A^+A = E$,其中 E 为 n 阶单位矩阵,A^+ 为 A 的厄密共轭. 不变矩阵元

$$\mathrm{d}\mu(g) = \left\{\prod_{\mu,\nu}^{n}\mathrm{d}(\mathrm{Re}A_{\mu\nu})\prod_{\mu,\nu}^{n}\mathrm{d}(\mathrm{Im}A_{\mu\nu})\right\},$$

亦即对于流体体积

$$V = \int\prod_{\mu,\nu}^{n}\mathrm{dRe}A_{\mu\nu}\int\prod_{\mu,\nu}^{n}\mathrm{dIm}A_{\mu\nu} = \prod_{\mu,\nu}^{n}\mathrm{Re}A_{\mu\nu} \cdot \prod_{\mu,\nu}^{n}\mathrm{Im}\ A_{\mu\nu},$$

其中 $\mathrm{Re}\ A_{\mu\nu}$ 与 $\mathrm{lm}\ A_{\mu\nu}$ 分别表示矩阵元 $A_{\mu\nu}$ 的实部与虚部. 但幺正条件

$$A + A^+ = E \to \sum_{\nu=1}^{n}(A^+)_{\mu\nu}(A)_{\mu\nu} = \delta_{\mu\nu}$$

$$\Rightarrow \sum_{\nu} A_{\nu\mu}^* A_{\nu\lambda} = \delta_{\mu\lambda}(\mu, \lambda = 1, \cdots, n),$$

当 $\lambda = \mu$ 时,上式 $= \sum_{\nu=1}^{n} A_{\nu\mu}^* A_{\nu\lambda} = 1 \Rightarrow \sum_{\nu=1}^{n}|A_{\nu\mu}|^2 = 1$,亦即 $|A_{\nu\mu}| \leqslant 1(\mu, \nu = 1, \cdots, n) \to \mathrm{Re}\ A_{\mu\nu}$ 与 $\mathrm{Im}\ A_{\mu\nu}$ 均有界. 因此,流形体积亦有限,$U(n)$ 群是紧密的.

定义 7.1.6　存在不变体积元,但群流形体积无限,这种群叫局部紧致群.

问题 7.1

1. 定义集合 $G = \{A \mid A$ 为 $n \times n$ 矩阵，且 $\det A \neq 0\}$，其中 $\forall\ A_{\mu\nu}(\mu, \nu = 1, 2, \cdots, n) \in \Omega(C)$，则集合记为 $GL(n, C)$；如 $\forall\ A_{\mu\nu}(\mu, \nu = 1, 2, \cdots, n) \in \Omega(R)$，则集合记为 $GL(n, R)$. 证明：$GL(n, C)$ 与 $GL(n, R)$ 均构成群. 它们的紧致性如何？

2. 设 $SL(n,C)$ 与 $SL(n,R)$ 的定义为

$SL(n,C) = \{A \mid A \in GL(n,C)$，且 $\det A = 1\}$；

$SL(n,R) = \{A \mid A \in GL(n,R)$，且 $\det A = 1\}$，

这里 SL 即特殊线性. 证明它们均构成群，并讨论其紧致性.

3. 定义集合 $SU(n) = \{A \mid A \in GL(n,C)$，且 $A^+ A = 1, \det A = 1\}$，这里 SU 即 Special Unitary，即特殊幺正，证明该集合构成群，并讨论其紧致性.

4. 定义 $O(n,C)$ 与 $SO(n,C)$ 为 $O(n,C) = \{A \mid A \in GL(n,C),\ \widetilde{A}A = E\}$；$SO(n, C) = \{A \mid A \in GL(n,C), \widetilde{A}A = E, \det A = 1\}$，这里 O 与 SO 表示正交与特殊正交. 证明它们构成群，并讨论其紧致性.

5. 若 $O(n,C)$ 与 $SO(n,C)$ 集合中，$\forall\ A_{\mu\nu} \in \Omega(R)$，则记为 $O(n,R)$ 与 $SO(n,R)$. 证明两集合依然构成群，并讨论其紧致性. 其中 $SO(n,C)$ 往往也记为 R_n，即 n 维转动群.

6. 定义集合 $Sp(2n,C)$ 为 $Sp(2n,C) = \{A \mid A \in GL(n,C)$，其中 J 为 $2n \times 2n$ 矩阵，证明任何 $\forall\ A \in Sp(n,C)$，则 $\det A = 1$，且集合 $Sp(2n,C)$ 构成群，称为辛群(注：$GL(n, C)$、$U(n)$、$O(n,C)$ 和 $Sp(2n,C)$ 统称典群).

7. 给出群 $SU(n)$ 的群流形，计算其群体积. [提示：考虑 $SU(n)$ 的自由参数个数]

§7.2　拓扑群及其表示

让我们先来举几个拓扑(紧致)群的常见实例.

例 7.2.1　有限群：任给一个有限元的群，对于离散拓扑来说，构成一个拓扑(紧致)群.

例 7.2.2　幺模复数群，所有的幺模复数$\{e^{i\theta}, 0 \leqslant \theta \leqslant 2\pi\}$ 在乘法运算下成一紧致群. 它是连通的，可交换的，以符号 S^1 表示之.

例 7.2.3　幺模四元数群是由所有能表成 $a + bi + cj + dk(a,b,c,d \in \mathbf{R})$ 的实四维向量，并赋以 $i^2 + j^2 + k^2 = -1,\ ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j$ 的双线性乘法所成的不可交换的体. 其中的幺模向量全体在上述乘法下成一个紧致群. 它是连通的，不可交换的，它在几何上可视为 $\mathbf{R}^4$ 中的三维单位球面，以 S^3 表示之.

例 7.2.4　n 维欧氏空间的正交变换群：设 $\mathbf{R}^n$ 是一个 n 维欧氏空间，则其上的所有

正交(亦即正交)变换构成一个拓扑群,叫做 n 阶正交群,以符号 $O(n)$ 表示之.

例 7.2.5　n 维酉空间的酉变换群:设 $\mathbf{C}^n$ 是一个 n 维酉空间,则其上所有的酉变换(即:使 $(gx,gy)=(x,y)$ 对任何 $x,y\in\mathbf{C}^n$ 恒成立的变换)构成一个拓扑群,叫做 n 阶酉群,以符号 $U(n)$ 表示之.不难看出 $U(1)=S^1$.

现在给出拓扑群和紧致群的定义.

定义 7.2.1　设 G 是一个非空集合,假如:

1)G 为一个群;

2)G 为拓扑空间;

3)G 中所具有的群的运算,$(a,b)\to a\cdot b; a\to a^{-1}(a,b\in G)$,

在拓扑空间中是连续的,那么就称 G 为拓扑群.

若在 2) 中加上紧致性要求,G 称为紧致拓扑群,简称为紧致群.

对于一个拓扑群 G 上给定的连续函数 $f(x)$,可以结合群上的右平移

$$\rho_a: G\to G,\quad \rho_a(x)=x\cdot a,$$

而得出新的函数 $f_a(x)=f(x\cdot a)$.

紧致群的一个重要特征是对于其上的连续函数 f,有一个自然的求平均值运算,它是一个满足下列条件的映射 $I: C(G)\to C$(或 R),其中 $C(G)$ 表示 C 上连续函数全体组成的集合,即

1) 不变性:$I(f_a)=i(f), f\in\mathbf{C}(G), a\in G$;

2) 线性性:$I(\lambda f+\mu g)=\lambda I(f)+\mu I(g),\quad f,g\in\mathbf{C}(G),\lambda,\mu\in\mathbf{C}$(或 $\mathbf{R}$);

3) 若 f 在 G 中处处非负,则 $I(f)\geqslant 0$,f 不恒等于零,则 $I(f)>0$;

4) 若 $f\equiv c$(常数),则 $I(f)=c$.

例 7.2.6　设 G 是一个有限群,则显然可以定义

$$I(f)=\frac{1}{|G|}\sum_{g\in G}f(g)\quad (|G|=G\text{ 的元素个数})$$

是 f 的平均值,它满足 1) ~ 4).

例 7.2.7　设 $G=S^{-1}$,则可以用积分来定义平均值如下:

$$I(f)=\frac{1}{2\pi}\int_0^{2\pi}f(e^{f\theta})\mathrm{d}\theta,$$

不难验证它也是满足 1) ~ 4) 的.

例 7.2.8　设 $G=S^3$,把它几何地想成 $\mathbf{R}^4$ 中的单位球面,则可用 $S^3(1)$ 上的体积元素 $\mathrm{d}\sigma$ 来定义平均值如下:

$$I(f)=\frac{1}{2\pi^2}\int_{S^3(1)}f(x)\mathrm{d}\sigma,$$

其中 $2\pi^2$ 是 $S^3(1)$ 的体积.不难看出它也自然满足上述四条.

定理 7.2.1 设 G 为一紧致群，$C(G)$ 为其上的所有复值（或实值）连续函数的集合，则满足性质 1) ～ 4) 的平均运算 $I: C(G) \to C$（或 R）唯一存在，称之为 G 上的（正规）不变积分，并用符号 $\int_G f(g)\mathrm{d}g$ 表示 $I(f)$.

下面我们就要运用"平均法"来系统地研讨紧致拓扑群的线性表示论. 在本节中，我们将以符号 G 表示一个任给的紧致拓扑群，而不再另加说明. 设 V 是一个复或实的向量空间，$GL(V)$ 是由 V 上的所有可逆线性变换所组成的群，叫做 V 的全线性群.

V 上线性变换全体组成的向量空间 $L(V,V)$ 自然与 C^n（或 R^n）同构，在 $L(V,V)$ 中引入 C^{n^2}（或 R^{n^2}）的拓扑结构，于是 $GL(V)$ 是 $L(V,V)$ 中开集，易见 $GL(V)$ 是一个拓扑群.

定义 7.2.2 若映射 $\varphi: G \to GL(V)$ 是拓扑群的同态映射（即，作为群的映射是同态，作为拓扑空间的映射是连续映射），称 φ 为 G 的一个线性表示，简称为表示. 通常也用符号 (G, V) 来表示之.

本节中将以不变积分所提供的平均法为主要手段来研讨 G 的线性表示.

定理 7.2.2 设 (G, V) 是一个复（实）表示，则 V 上必存在一个 G— 不变的酉积（内积），即 $(gx, gy) = (x, y)$，对 $\forall\, g \in G$, $x, y \in V$ 恒成立.

证明 设 $< x, y >$ 是 V 上的一个任选的酉积（内积），令

$$(x,y) = \int_G < gx, gy > \mathrm{d}g,$$

则对 $\forall\, a \in G$，均有

$$(ax,ay) = \int_G < gax, gay > \mathrm{d}g = \int_G < gx, gy > \mathrm{d}g = (x,y),$$

所以 (x, y) 是 G— 不变的酉积（内积）.

推论 7.2.3 设 $G \subset GL(n,C)$（n 维复向量空间上的全线性群）是一个紧致子群，则必存在一个适当的 $A \in GL(n,C)$，使得 $AGA^{-1} \subset U(n)$. 因此，$U(n)$ 是 $GL(n,C)$ 的一个极大紧致子群，而 $GL(n,C)$ 的任何极大紧致子群都和 $U(n)$ 共轭.

证明 设 $\{e_1, \cdots, e_n\}$ 是 C^n 在原给酉积 $<,>$ 下的标准正交基，$\{a_1, \cdots, a_n\}$ 是在上述 G— 不变酉积 $(,)$ 下的一组标准正交基，A 是将 a_i 映到 $e_i (i = 1, \cdots, n)$ 的那个在 $GL(n,C)$ 中的元素，即得所欲证.

定义 7.2.3 (G, V) 和 (G, W) 之间若存在一个和 G 的作用可交换的线性同构

$$A: V \to W, \text{即 } A(gx) = gA(x),$$

则称 (G, V) 和 (G, W) 等价（或 G— 同构），记为 $(G, V) \cong (G, W)$.

同样，$\varphi: G \to GL(V)$ 和 $\psi: G \to GL(W)$ 是等价的充要条件是：存在同构 $A: V \to W$，使得 $\sigma_A \circ \varphi = \psi$，其中 $\sigma_A: GL(V) \to GL(W)$ 的定义是 $\sigma_A(B) = ABA^{-1}, B \in GL(V)$.

定义 7.2.4　对于(G, V),若有一个子空间 $U \subset V$ 在 G 的作用下不变,即

$$G \circ U = \{g \circ x, g \in G, x \in U\} \subset U,$$

则称 U 为 G— 不变子空间.

显然有,$\{0\}$ 和 V 本身是 G— 不变的. 今后在不致发生混淆的情况下,G— 不变子空间简称为不变子空间.

定义 7.2.5　若 $\{0\}$ 和 V 是(G, V) 仅有的不变子空间,则称(G, V) 为不可约表示;否则叫可约表示.

下面我们建立线性表示的几种常用的运算:

1) **和**:设$(G, V_i)(i = 1, 2)$是 G 的两个线性表示,我们可以在 $V_1 \oplus V_2$ 上赋以 G 的作用:

$$g(x, y) = (gx, gy), x \in V_1, y \in V_2,$$

这个新的表示叫做原来两个表示之和,记为$(G, V_1) \oplus (G, V_2)$. 若用 $\varphi_i : G \to GL(V_i)$ 来记线性表示,则它们的和记为

$$\varphi_1 \oplus \varphi_2 : G \to GL(V_1 \oplus V_2).$$

2) **对偶**:设(G, V)是一个线性表示,V^* 表示 V 的对偶空间(即:V 上所有的线性函数组成的向量空间),在 V^* 上可如下规定 G 的作用 gf,使得

$$< g \circ f, x > = < f, g^{-1}x >,$$

其中 $f \in V^*$, $x \in V$, $g \in G$, $< f, x > = f(x)$.

容易验证,上述规定构成 G 到 V^* 上的一个线性表示,称之为对偶表示,记为(G, V^*). 若用 $\varphi: G \to GL(V)$ 来表示,则 φ 的对偶表示记为

$$\varphi^* : G \to GL(V^*).$$

3) **张量积**:把 2) 中的规定推广到多线性函数,设 $L(V_1, V_2)$,C(或 R)是 V_1,V_2 上所有双线性函数构成的向量空间,

$$\varphi_i : G \to GL(V_i), (i = 1,2)$$

是 G 在 V_1 及 V_2 上的表示.

规定$(\varphi_1, \varphi_2)^* : G \to GL(L(V_1, V_2, C(\text{或} R)))$ 如下:

$$(g \circ f)(x_1, x_2) = f(g^{-1}x_1, g^{-1}x_2), (f \in L(V_1, V_2, C(\text{或} R)).$$

在向量空间的张量积中,我们用张量积把多线性函数归于单线性函数的讨论. 我们有

$$L(V_1, V_2, C) \cong L(V_1 \otimes V_2, C) = (V_1 \otimes V_2)^*.$$

再由对偶关系 $(L(V_1, V_2, C))^* \cong V_1 \otimes V_2$,我们规定 φ_1,φ_2 的张量积 $\varphi_1 \otimes \varphi_2$ 为:

$$\varphi_1 \otimes \varphi_2 = ((\varphi_1, \varphi_2)^*)^*.$$

容易验证:

$$g(\mu\otimes\nu)=g\cdot\mu\otimes g\cdot\nu,\quad \mu\in V_1,\ \nu\in V_2.$$

4) 设 $\varphi_i: G\to GL(V_i)(i=1,2)$ 分别是 G 到 V_i 上的线性表示. $L(V_1, V_2)$ 是由所有的 V_1 到 V_2 上的线性变换构成的向量空间. 现在在 $L(V_1, V_2)$ 上赋以 G 的作用如下:

$$g\cdot A=\varphi_2(g)A\varphi_1,(g)^{-1}),\ A\in L(V_1, V_2)$$

亦即图 7.5 是可交换的. 也可写为

$$(g\cdot A)(x)=g\cdot A\,g^{-1}(x),\ x\in V_1$$

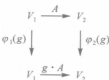


图 7.5

由于 $L(V_1, V_2)\cong V_1\otimes V_2^*$, 可以证明上述表示等价于 $\varphi_1\otimes\varphi_2^*$. 利用上述诸运算, 我们可以由简单的表示来构造较为复杂的表示, 又可把较为复杂的表示进行分解. 此外, 表示的和与张量积均可推广到多个的情况. 利用张量积的概念, 对一个给定的表示 $\varphi: G\to GL(V)$, 可定义张量幂 $\varphi,\varphi: G\to GL(V)$. 更一般地, $\varphi^r: G\to GL(\otimes V)$.

定义 7.2.6　若 $(G, V)\cong(G, V_1)\cdots(G, V_k)$, 其中右边的每个 (G, V_i) 都是不可约的, 则称 (G, V) 是完全可约的(其中 $i=1,\cdots,k$).

由此定义和定理 7.2.2 还有如下重要结论:

推论 7.2.4　任何紧致群的表示 (G, V) 都是完全可约的.

证明　设 V_1 是 V 的非平凡的不变子空间, V 上存在 G— 不变内积, 因此 V_1 关于这个内积的正交补 $V_1^\perp$ 也是不变的, 从而 $(G, V)\cong(G, V_1)\oplus(G, V_1^\perp)$. 若 (G, V_1) 或 $(G, V_1^\perp)$ 仍有非平凡不变子空间, 可继续分解下去, 直至不可分解为止. 这就完成了所求的分解.

上述事实表明: 对紧致群的线性表示的探讨, 基本上都归于不可约线性表示来研究. 而下述引理则是研讨不可约线性表示的基本工具.

Schur 引理　设 $\varphi: G\to GL(V)$ 和 $\psi: G\to GL(W)$ 是两个不可约表示, 而 $A\in L(V, W)$. 记

$$A\cdot\varphi(G)=\{A\cdot\varphi(g)\,|\,g\in G\},\ \psi(G)\cdot A=\{\psi(g)\cdot A\,|\,g\in G\},$$

若 $A\cdot\varphi(G)=\psi(G)\cdot A$ 则必有 $A=0$ 或 A 是可逆的.

证明　由上述假设不难看出 $\mathrm{Ker}A$ 和 $\mathrm{Im}A$ 分别是 V 和 W 中的 G— 不变子空间. 再由 φ 和 ψ 的不可约性即得 $\mathrm{Ker}A$ 和 $\mathrm{Im}A$ 只有下列两种可能:

$$\mathrm{Ker}A=V \text{ 且 } \mathrm{Im}A=\{0\}, \text{即 } A=0;$$

或者

$$\mathrm{Ker}A=\{0\} \text{ 且 } \mathrm{Im}A=W, \text{即 } A \text{ 是可逆的}.$$

当 $\varphi=\psi$ 而且是复不可约表示时, 还有下述特殊形式:

Schur 引理的特殊形式　设 $\varphi: G\to GL(V)$ 为一个复不可约表示, 而且 $A\in L(V, W)$ 满足 $\varphi(g)\cdot A=A\cdot\varphi(g), g\in G$, 则必存在一个适当复数 $\lambda_0\in C$, 使得 $A=\lambda_0 I$.

证明　显然 $\varphi(g)(A-\lambda I)=(A-\lambda I)\cdot\varphi(g)$，对于所有的 $g\in G$ 也成立. 再有，在复数域中必存在一个 λ_0，使得 $A-\lambda_0 I$ 是不可逆的，所以由上述引理即得，$A-\lambda_0 I=0$，亦即 $A=\lambda_0 I$.

定理 7.2.5　设 $\varphi:G\to GL(V)$ 和 $\psi:G\to GL(W)$ 是两个不等价的复不可约表示. 在 V,W 上各取一个 G— 不变酉积，而且各取一组标准正交基，则可用酉矩阵表达 $\varphi(g)$ 和 $\psi(g)$，$\varphi(g)=(\varphi_{ij}(g))$，$\psi(g)=(\psi_{kl}(g))$，

它们之间具有下述正交关系：

$$\int_G \psi_{kl}(g)\circ\overline{\varphi_{ij}(g)}\mathrm{d}g=0,$$

$$\int_G \varphi_{kl}(g)\circ\overline{\varphi_{ij}(g)}\mathrm{d}g=\frac{1}{\dim\varphi}\delta_{ki}\delta_{lj},$$

其中 $\dim\varphi$ 是不可约表示 φ 的表示空间的维数.

证明　结合 G 在 V 和 W 上的作用，在前面我们已经定义了 G 在 $L(V,W)$ 上的诱导作用，即

$$g\cdot A=\psi(g)A\,\varphi(g)^{-1},\ A\in L(V,W).$$

再运用不变积分，求轨道 $G\cdot A=\{g\cdot A\,|\,g\in G\}$ 的平均值(亦即其重心)，得到 $\overline{A}=\int_G g\cdot A\mathrm{d}g$，不难看出，$\overline{A}$ 肯定是一个在 G 的作用下不变的元素，事实上，

$$a\cdot\overline{A}=\int_G(ag)\cdot A\mathrm{d}g=\int_G g\circ A\mathrm{d}g=\overline{A}.$$

上式表明，$\psi(a)\overline{A}\varphi(a)^{-1}=\overline{A}$ 或 $\psi(a)\overline{A}=\overline{A}\varphi(a)$，再用 Schur 引理便得出 $\overline{A}=0$(因为 $\overline{A}$ 若可逆，则 φ 和 ψ 就是等价的了!)，而 A 是 $L(V,W)$ 中的任意元素. 现在我们取 $A=E_{ki}$，即 $L(V,W)$ 中把 V 中第 i 个基向量映射到 W 中第 k 个基向量，而其他均映为零的那个线性映射，则

$$E_{ki}=\int_G(\psi_{kl}(g))E_{ki}(\varphi_{ij}(g))^{-1}\mathrm{d}g=0.$$

把上式用矩阵算法直接写出，就得到

$$\int_G\psi_{kl}(g)\circ\overline{\varphi_{ij}(g)}\mathrm{d}g=0.$$

若取 $B\in L(V,V)$，则类似可得

$$\overline{B}=\int_G g\circ B\mathrm{d}g=\int_G\varphi(g)B\varphi(g)^{-1}\mathrm{d}g=\lambda(B)\circ I,$$

其中 $\lambda(B)$ 是一个由 B 所确定的复数. 另一方面，又有

$$Tr(\overline{B})=Tr\int_G\varphi(g)B\varphi(g)^{-1}\mathrm{d}g=\int_G Tr(\varphi(g)B\varphi(g)^{-1})\mathrm{d}g=\int_G TrB\mathrm{d}g=TrB,$$

也就是说，$TrB=Tr\overline{B}=\dim\varphi\circ\lambda(B)$，所以 $\lambda(B)=\dfrac{1}{\dim\varphi}\circ TrB$.

同样地，取 $B = E_{ij}$ 即得

$$E_{ij} = \int_G \varphi(g) E_{ij} \varphi(g)^{-1} \mathrm{d}g = \delta_{ij} \circ \frac{1}{\dim\varphi} \circ I.$$

用矩阵算法就得 $\int_G \varphi_{kl}(g) \circ \overline{\varphi_{ij}} \mathrm{d}g = \frac{1}{\dim \varphi} \delta_{ik} \delta_{jl}$.

定义 7.2.7　对于给定的复(实)表示 $\varphi: G \to GL(V)$，令 $\chi_\phi(g) = T_r \varphi(g)$，$g \in G$，称 χ_ϕ 为表示 φ 的特征函数.

不难看出，$\varphi \cong \psi \Rightarrow \chi_\phi = \chi_\varphi$.

特征函数有以下简单性质：

$$\chi_{\phi \oplus \varphi} = \chi_\phi + \chi_\varphi; \chi_{\phi \otimes \varphi} = \chi_\phi \cdot \chi_\varphi.$$

推论 7.2.6　若 φ 和 ψ 是 G 的两个不等价的复不可约表示，则

$$\int_G \chi_\varphi(g) \cdot \overline{\chi_\psi(g)} \mathrm{d}g = 0, \int_G \chi_\varphi(g) \cdot \overline{\chi_\varphi(g)} \mathrm{d}g = 1.$$

证明

$$\int_G \chi_\varphi(g) \cdot \overline{\chi_\psi(g)} \mathrm{d}g = \int_G \left(\sum_{i=1}^n \varphi_{ij}(g)\right) \cdot \sum_{k=1}^m \overline{\varphi_{kk}(g)} \mathrm{d}g$$

$$= \sum_{i=1}^n \sum_{k=1}^m \int_G \varphi_{ii}(g) \cdot \overline{\psi_{kk}(g)} \mathrm{d}g = 0,$$

而

$$\int_G \chi_\varphi(g) \cdot \overline{\chi_\varphi(g)} \mathrm{d}g = \int_G \left(\sum_{i=1}^n \varphi_{ii}(g)\right) \cdot \left(\sum_{j=1}^n \overline{\varphi_{jj}(g)}\right) \mathrm{d}g$$

$$= \sum_{i,j=1}^n \int_G \varphi_{ii}(g) \cdot \overline{\varphi_{jj}(g)} \mathrm{d}g = \sum_{i,j=1}^n \frac{\delta_{ij}}{n} = 1.$$

设 ρ 是 G 的一个任意复表示. 因为紧致群的任何表示都是完全可约的，所以我们把 ρ 表示为不可约表示的和，叫做 ρ 的完全分解，$\rho = \bigoplus \Sigma \varphi_i$，其中 φ_i 是不可约的. 通常我们把等价的不可约表示写在一起，即改写为 $\rho = \bigoplus \Sigma m_i \varphi_i$，其中 φ_i 是相异的不可约表示，m_i 是 ρ 的完全分解中含有的与 φ_i 等价的不可约表示的重数. 或者，我们还可以引进符号 $m(\rho, \varphi)$，表示在 ρ 的完全分解中含有与不可约表示 φ 等价者的重数，则 $\rho = \bigoplus \Sigma_\varphi m(\rho, \varphi)\varphi$，其中 φ 遍历 G 的所有互不等价的复不可约表示. 当然，在上式中，只有有限个 $m(\rho, \varphi)$ 不等于零. 显然有 $\rho_1 \cong \rho_2 \Leftrightarrow$ 对于 G 的任何复不可约表示 φ，$m(\rho_1, \varphi) = m(\rho_2, \varphi)$ 恒成立.

定理 7.2.7

1) $m(\rho, \varphi) = \int_G \chi_\rho(g) \cdot \overline{\chi_\varphi(g)} \mathrm{d}g$.

2) $\rho_1 \cong \rho_2 \Leftrightarrow \chi_{\rho_1} = \chi_{\rho_2}$，也就是说，$\chi_{\rho_1}(g) = \chi_{\rho_2}(g)$ 对 $\forall\, g \in G$ 恒成立.

3) ρ 是不可约的充要条件是 $\int_G |\chi_\rho(g)|^2 \mathrm{d}g = 1$.

证明　显然有 $\chi_\rho(g)=\sum_\varphi m(\rho,\varphi)\chi_\varphi(g)$. 设 φ_0 是 G 的一个任意给定的复不可约表示,则

$$\int_G \chi_\rho(g)\cdot\overline{\chi_{\varphi_0}(g)}\mathrm{d}g=\sum_\varphi m(\rho,\varphi_0)\int_G \chi_\varphi(g)\cdot\overline{\chi_{\varphi_0}(g)}\mathrm{d}g.$$

上述和式中的诸积分中,只有当 $\varphi=\varphi_0$ 时为 1,其他各项均为零. 所以有

$$\int_G \chi_\rho(g)\cdot\overline{\chi_{\varphi_0}(g)}\mathrm{d}g=m(\rho,\varphi_0).$$

但是 φ_0 是 G 的任给的复不可约表示,所以 $\rho_1\cong\rho_2\Leftrightarrow\chi_{\rho_1}=\chi_{\rho_2}.g\in G$ 不难算出

$$\int_G \chi_\rho(g)\cdot\overline{\chi_\rho(g)}\mathrm{d}g=\sum_\varphi[m(\rho,\varphi)]^2,$$

因此 ρ 是复不可约的充要条件是$\int_G \chi_\rho(g)\cdot\overline{\chi_\rho(g)}\mathrm{d}g=1$.

§7.3　$L_2(G)$ 空间

定义 7.3.1　紧致群 G 上的可积函数 f(即$\int_G f(g)\mathrm{d}g$ 存在,其中 $\mathrm{d}g$ 是由 G 上不变积分决定的测度),若$\int_G |f|^2\mathrm{d}g<+\infty$,则称 f 是平方可积的,简称为 L_2- 函数. 两个 L_2-函数 f_1 和 f_2 称为是等价的,如果$\int_G |f_1-f_2|^2\mathrm{d}g=0$,也就是说,$f_1$, f_2 的值在 G 上几乎处处相等.

由所有的 G 上的 L_2- 函数的等价类所构成的向量空间,以符号 $L_2(G)$ 表之. 我们还以下式定义其上的内积:

$$<f_1,f_2>=\int_G f_1(g)\,\overline{f_2(g)}\mathrm{d}g.$$

不难验证上式的确定义了 $L_2(G)$ 上的一个酉积,这样就赋以 $L_2(G)$ 一个自然的 Hilbert 空间的结构.

令 $IR(G)$ 是由 G 的所有复不可约表示的等价类所组成的集合,则

$$\{\varphi_{ij}(g),\ \varphi(g)\}=\{\varphi_{ij}(g)\},\quad \varphi\in IR(G)$$

是 $L_2(G)$ 中的一组正交向量,而且

$$|\phi_{ij}(g)|_{L_2}^2=1/\dim\varphi.$$

其实,还可以进一步证明上面这一组向量已构成 $L_2(G)$ 空间的一组基底,这就是 Peter-Weyl 定理.

$\{\varphi_{ij}(g),\ \varphi(g)\}=\{\varphi_{ij}(g)\},\varphi\in IR(G)$ 组成 Hilbert 空间 $L_2(G)$ 的一组基底.

定义 7.3.2 在 G 上的每个共轭类上取等值的 L_2- 函数，叫做 G 上的中心函数. 若以 $G/G/\widetilde{A}d$ 表示由 G 的所有共轭类所构成的商空间，并且赋以适当的测度 $\mathrm{d}\sigma$，使得

$$\int_{G/\widetilde{A}d} f\mathrm{d}\sigma = \int_G (f\circ\pi)\mathrm{d}g,$$

其中 $\pi: G\to G/\widetilde{A}d$ 是自然映射，$f: G/\widetilde{A}d\to C$(或 R)，则 G 上的所有中心函数所构成的子空间和 $L_2(G/\widetilde{A}d)$ 同构. 换句话说，映射

$$\pi^*: L_2(G/\widetilde{A}d)\to L_2(G)\qquad \pi^* f = f\cdot\pi$$

是一个由 $L_2(G/\widetilde{A}d)$ 到上述子空间的同构.

把上面两定理结合起来，即得

定理 7.3.1 $\{x_\varphi|\varphi\in IR(G)\}$ 组成 $L_2(G/\widetilde{A}d)$ 的一组标准正交基.

定义 7.3.3 设 (G_1,V_1) 和 (G_2,V_2) 是两个给定的复(实)表示，则存在唯一的一个复(实)表示 $(G_1\times G_2, V_1\otimes_2 V_2)$ 或 $(G_1\times G_2, V_1\otimes_R V_2)$:

$$(g_1,g_2)x_1\otimes x_2 = g_1x_1\otimes g_2x_2,(g_i\in G_i, x_i\in V_i(i=1,2).$$

我们把它叫做 (G_1,V_1) 和 (G_2,V_2) 的外张量积，以符号 $(G_1,V_1)\hat{\otimes}(G_2,V_2)$ 表之. 同样，我们用 $\varphi_1\hat{\otimes}\varphi_2$ 表示

$$\varphi_1: G_1\to GL(V_1) \text{ 和 } \varphi_2: G_2\to GL(V_2)$$

的外张量积，

$$\varphi_1\hat{\otimes}\varphi_2: G_1\times G_2\longrightarrow GL(V_1\otimes V_2).$$

定理 7.3.2 $IR(G_1\otimes G_2) = \{\varphi_1\hat{\otimes}\varphi_2; \varphi_1\in IR(G_1), \varphi_2\in IR(G_2)\}$.

证明 先证 $\chi_{\varphi_1\hat{\otimes}\varphi_2}(g_1,g_2) = \chi_{\varphi_1}(g_1)\cdot\chi_{\varphi_2}(g_2)$，对于任给的 $g_1\in G$ 和 $g_2\in G$ 恒成立. 我们可以在 V_i 上取定 G_i— 不变的酉积，对于任意给定的 $g_i\in G_i$，$\varphi_i(g_i)$ 是 V_i 上的酉变换 $(i=1,2)$，所以分别存在 V_1 和 V_2 中的正交基 $\{e_1,\cdots,e_n\}$ 和 $\{e'_1,\cdots,e'_m\}$，它们分别都是 $\varphi_1(g_1)$ 和 $\varphi_2(g_2)$ 的特征向量，即:

$$\begin{cases}\varphi_1(g_1)e_k = \lambda_k e_k, & 1\leqslant k\leqslant n;\\ \varphi_2(g_2)e'_l = \mu_l e_l, & 1\leqslant l\leqslant m.\end{cases}$$

而 $\{e_k\otimes e'_l; 1\leqslant k\leqslant n, 1\leqslant l\leqslant m\}$ 显然构成 $V_1\otimes V_2$ 中一组正交基，而且由 $\varphi_1\hat{\otimes}\varphi_2$ 的定义

$$\varphi_1\hat{\otimes}\varphi_2(g_1,\ g_2)e_k\otimes e'_l = (\lambda_k,\ \mu_l)e_k\otimes e'_l,$$

所以

$$\chi_{\varphi_1\hat{\otimes}\varphi_2}(g_1,g_2) = \sum_{l=1}^{m}\sum_{k=1}^{n}\lambda_k\mu_l = (\sum_{k=1}^{n}\lambda_k)(\sum_{l=1}^{m}\mu_l) = \chi_{\varphi_1}(g_1)\cdot\chi_{\varphi_2}(g_2),$$

由上式即得

$$\int_{G_1\times G_2}|\chi_{\varphi_1\hat{\otimes}\varphi_2}(g_1,g_2)|^2\mathrm{d}g_1\cdot\mathrm{d}g_2=\int_{G_1\times G_2}|\chi_{\varphi_1}(g_1)|^2\cdot|\chi_{\varphi_2}(g_2)|^2\mathrm{d}g_1\mathrm{d}g_2$$
$$=\int_{G_1}|\chi_{\varphi_1}(g_1)|^2\mathrm{d}g_1\cdot\int_{G_2}|\chi_{\varphi_2}(g_2)|^2\mathrm{d}g_2=1.$$

这也就证明了 $\varphi_1\widetilde{\otimes}\varphi_2(\varphi_1\in LR(G_1),\varphi_2\in LR(G_2))$ 是 $G_1\times G_2$ 的复不可约表示. 再有，设 ψ_1,ψ_2 也分别是 $LR(G_1)$ 和 $LR(G_2)$ 中的元素，则有

$$\begin{aligned}\langle\chi_{\varphi_1\otimes\varphi_2},\chi_{\psi_1\otimes\psi_2}\rangle&=\int_{G_1\times G_2}\chi_{\varphi_1\otimes\varphi_2}\circ\overline{\chi_{\psi_1\otimes\psi_2}}\mathrm{d}g_1\mathrm{d}g_2\\&=\int_{G_1\times G_2}\chi_{\varphi_1}(g_1)\circ\chi_{\varphi_2}(g_2)\circ\overline{\chi_{\psi_1}(g_1)}\circ\overline{\chi_{\psi_2}(g_2)}\mathrm{d}g_1\mathrm{d}g_2\\&=\int_{G_1}\chi_{\varphi_1}(g_1)\,\overline{\chi_{\psi_1}(g_1)}\mathrm{d}g_1\circ\int_{G_2}\chi_{\varphi_2}(g_2)\,\overline{\chi_{\psi_2}(g_2)}\mathrm{d}g_2\\&=\langle\chi_{\varphi_1},\chi_{\psi_1}\rangle\circ\langle\chi_{\varphi_2},\chi_{\psi_2}\rangle,\end{aligned}$$

所以 $\{\chi_{\varphi_1\otimes\varphi_2};\varphi_1\in IR(G_1),\varphi_2\in IR(G_2)\}$ 构成了

$$L_2(G_1/\widetilde{A}d\times G_2/\widetilde{A}d)\subseteq L_2(G_1\times G_2/\widetilde{A}d)$$

的一组正交基. 这也就证明了上述集合业已构成 $LR(G_1\times G_2)$ 的全体，亦即 $G_1\times G_2$ 的任何复不可约表示都能表为 $\varphi_1\widetilde{\otimes}\varphi_2$ 形式.

群的运算自然地给出了 $G_1\times G_2$ 在 G 本身上的左、右平移变换，即下述变换：

$$G\times G\to G:(g_1,g_2)x=g_1\circ x\circ g_2^{-1}.$$

这个变换诱导出下述 $G\times G$ 在 $L_2(G)$ 上的变换：

$$(G\times G)\times L_2(G)\to L_2(G):[(g_1,g_2)f](x)=f(g_1^{-1}xg_2).$$

易证：上述变换决定了 $G\times G$ 在 Hilbert 空间 $L_2(G)$ 上的一个线性表示，不难证明，对于任何 $\varphi\in IR(G)$，由 $(\dim\varphi)^2$ 个表示函数 $\{\varphi_{ij}(g)\}$ 所张成的子空间是 $G_1\times G_2$—不变的，而且在其上的作用等价于 $\varphi^*\widetilde{\otimes}\varphi$，其中 φ^* 是 φ 的对偶表示. 事实上，设 φ 对于基 $e_1,\cdots,e_n$ 的表示函数为 $\varphi_{ij}(g)(1\leqslant i,j\leqslant n)$，按定义

$$[(g_1,g_2)\varphi_{ij}](g)=\varphi_{ij}(g_1^{-1}gg_2).$$

另一方面，由 $\varphi(g_1^{-1}gg_2)=\varphi(g_1^{-1})\varphi(g)\varphi(g_2)$ 可知，

$$\varphi_{ij}(g_1^{-1}gg_2)=\sum_{k,l}\varphi_{ik}(g_1^{-1})\varphi_{kl}(g)\varphi_{lj}(g_2)=\sum_{k,l}\varphi_{ik}(g_1^{-1})\varphi_{lj}(g_2)\varphi_{kl}(g).$$

因此，

$$[(g_1,g_2)\varphi_{ij}](g)=\sum_{k,l}\varphi_{ik}(g_1^{-1})\varphi_{lj}(g_2)\varphi_{kl}(g).$$

上式说明由 $\{\varphi_{ij}(g)\}$ 张成的子空间是 $G\times G$ 不变的. 为证明它与 $\varphi^*\widetilde{\otimes}\varphi$ 等价，可直

接计算 $\varphi^* \widetilde{\otimes} \varphi$. 由定义

$$\begin{aligned}\varphi^* \widetilde{\otimes} \varphi(g_1, g_2)(e_i^* \otimes e_j) &= \varphi^*(g_1)e_i^* \otimes \varphi(g_2)e_j \\ &= \sum_k \varphi_{ik}(g_1^{-1})e_k^* \otimes \sum_l \varphi_{lj}(g_2)e_l \\ &= \sum_{k,l} \varphi_{ik}(g_1^{-1}) \cdot \varphi_{lj}(g_2)e_k^* \otimes e_l.\end{aligned}$$

由于 $\{\varphi_{ij}(g)\}$ 是此子空间的基，而 $\{e_k^* \otimes e_l\}$ 是 $V^* \otimes V$ 的基，比较上面两式，上述等价性是明显的.

总结本节的讨论，即有

$$L_2(G) \cong \oplus \sum_{\varphi \in IR(G)} V(\varphi^*) \otimes_G V(\varphi),$$

其中 G 在 $V(\varphi^*) \otimes_G V(\varphi)$ 上的作用是 $\varphi^* \widetilde{\otimes} \varphi$.

现在让我们举几个实例，来看一看前面理论的一些初步用法.

1. Abel 群

设 G 为一个紧致可换群，φ 是 G 的一个复不可约表示，则不难用 Schur 引理的特殊形式证明 $\dim\varphi = 1$.

事实上，因为 G 是可换的，我们可以取 $A = \varphi(g_0)$，其中 g_0 是 G 中任意给定的元素. 则有

$$\varphi(g) \cdot \varphi(g_0) = \varphi(g_0 \cdot g_0) = \varphi(g_0) \cdot \varphi(g)$$

对所有 $g \in G$ 恒成立. 所以由引理可知，存在一个适当的 $\lambda(g_0)$，使得 $\varphi(g_0) = \lambda g_0 \cdot I$，其中 I 是表示空间上的恒等变换. 换句话说，

$$\varphi(G) = \{\varphi(g_0) \mid g_0 \in G\} \subset \{\lambda I : \lambda \in \mathbf{C}\}.$$

另一方面，显然有，表示空间 V 的任何子空间都是 $\{\lambda I : \lambda \in \mathbf{C}\}$ 的不变子空间，当然也是它的一部分 ——$\{\varphi(g_0) \mid g_0 \in G\} = \varphi(G)$ 的不变子空间. 但是 φ 假设为复不可约的，所以 V 除了 $\{0\}$ 和本身之外，不能再有其他的子空间了. 这种情形只有一种可能，就是 $\dim\varphi = \dim_{\mathbf{C}} V = 1$.

2. $G = S^1 = \{e^{i\theta}; 0 \leqslant \theta \leqslant 2\pi\}$

S^1 是一个紧致可换群，由 1)，它的任何复不可约表示 φ 都是一维的，即

$$\varphi: S^1 \to U(1) = S^1.$$

令

$$\varphi_n: S^1 \to S^1, \varphi_n: (e^{i\theta}) = e^{in\theta},$$

其中 n 是一个取定的整数. 容易看出, φ_n 是一个同态映射.

另一方面,设 $\varphi: S^1 \to S^1$ 是任取的一个同态映射,则不难证明: φ 必然与上述 φ_n 之一等价.

在数学分析中,我们熟知 $\{e^{in\theta}; n \in \mathbf{Z}\}$ 构成了 $L_2(S^1)$ 的一组正交基. 这也就是 Peter-Weyl 定理在 $G = S^1$ 下的形式. 所以 Peter-Weyl 定理其实就是上述傅氏级数的基本事实在紧致群范围中的深刻推广.

3. $G = S^3$ = 幺模四元数集合

我们先把四元数体表示成一个二维复空间,即:

$$Q = \{X = z_1 + jz_2; z_1, z_2 \in \mathbf{C}\} \cong C^2,$$

则 S^3 中的任一元素就可写成 $q = a + jb$, 其中 $a, b \in \mathbf{C}, a\bar{a} + b\bar{b} = |q|^2 = 1$. 对于这样一个给定的 q, 就对应有一个 $Q \cong C^2$ 上的线性变换: $X \to qX$, 其矩阵为 $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$, 或者写为 $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} az_1 - bz_2 \\ bz_1 + \bar{a}z_2 \end{pmatrix}$.

上述线性变换: $\begin{cases} z_1 \longmapsto az_1 - \bar{b}z_2, \\ z_2 \longmapsto bz_1 - \bar{a}z_2 \end{cases}$

就给出 S^3 在由 z_1, z_2 的 k 次齐次多项式所构成的线性空间上的一个线性表示,其定义如下: 设 f 是 z_1, z_2 的 k 次齐次多项式,规定

$$(q \circ f)(z_1, z_2) = f(az_1 - \bar{b}z_2, bz_1 + \bar{a}z_2), \ q = a + jb,$$

我们将以 φ_k 记这个复表示,它的维数是 $k + 1$.

定理 7.3.3　对于任给的 $k = 0, 1, 2, \cdots$, 上述 S^3 的复线性表示都是不可约的,而且 $IR(S^3) = \{\phi_k; k = 0, 1, 2, \cdots\}$.

证明　现在让我们把 Q 想成一个四维实向量空间. 这样,对于 S^3 中的任一元素 q, 就得到 R^4 的一个变换: $X \to qXq^{-1}$, 它是 R^4 上保持实数轴不动的一个正交变换,称之为共轭变换或伴随变换,所以 S^3 的伴随变换也可以看成一个以实数轴为不动点的 $SO(3)$ 旋转. 因此, S^3 中包含 $e^{i\theta}$ 的那个共轭类就是一个由垂直于实轴的三维超平面 S^3 所截出来的二维球面 S^2, 其半径为 $\sin\theta$, 其面积为 $4\pi\sin^2\theta$(图 7.6). 令以 χ_k 表示 χ_{ϕ_k}. 因为 χ_k 在上述共轭类上取等值,即

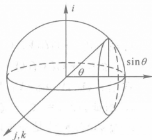


图 7.6

$$\chi_k(ge^{i\theta}g^{-1}) = \chi_k(e^{i\theta}),$$

所以有

$$\begin{aligned}\int_G \chi_k \overline{\chi_k} \mathrm{d}g &= \frac{1}{2\pi^2}\int_{S^3(1)} \chi_k \overline{\chi}_k \mathrm{d}\sigma \\ &= \frac{1}{2\pi^2}\int_0^{\pi} \chi_k(\mathrm{e}^{i\theta})\,\overline{\chi_k(\mathrm{e}^{i\theta})}(4\pi\sin^2\theta)\mathrm{d}\theta \\ &= \frac{1}{2\pi}\int_0^{\pi} \chi_k(\mathrm{e}^{i\theta})\,\overline{\chi_k(\mathrm{e}^{i\theta})}(\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta})\,\overline{(\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta})}\mathrm{d}\theta \\ &= \frac{1}{4\pi}\int_0^{2\pi} |\chi_k(\mathrm{e}^{i\theta})\circ(\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta})|^2\mathrm{d}\theta.\end{aligned}$$

再者，由 φ_k 的定义以及由 $\mathrm{e}^{i\theta}\in S^3$ 所决定的线性变换是

$$z_1 \longmapsto \mathrm{e}^{i\theta}z_1,\ z_2 \longmapsto \mathrm{e}^{-i\theta}z_2,$$

因此不难看出，单项式 $z_1^k, z_1^{k-1}z^2, \cdots, z^1 z_2^{k-1}, z_2^k$ 都是 $\varphi_k(\mathrm{e}^{i\theta})$ 的特征向量，而且相应的特征值分别是 $\mathrm{e}^{ik\theta}, \mathrm{e}^{i(k-2)\theta}, \cdots, \mathrm{e}^{-i(k-2)\theta}, \mathrm{e}^{-ik\theta}$. 所以

$$\begin{aligned}\chi_k(\mathrm{e}^{i\theta})(\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}) &= (\mathrm{e}^{ik\theta}+\mathrm{e}^{i(k-2)\theta}+\cdots+\mathrm{e}^{-i(k-2)\theta}+\mathrm{e}^{-ik\theta})\times(\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}) \\ &= (\mathrm{e}^{i(k+1)\theta}-\mathrm{e}^{-i(k+1)\theta}).\end{aligned}$$

将下式代入上式，便得出

$$\int_G |\chi_k|^2\mathrm{d}g = \frac{1}{4\pi}\int_0^{2\pi} |\mathrm{e}^{i(k+1)\theta}-\mathrm{e}^{-i(k+1)\theta})|^2\mathrm{d}\theta = 1.$$

这也就证明了 φ_k 是复不可约的，再因为

$$\{\chi_k(\mathrm{e}^{i\theta})(\mathrm{e}^{i\theta}-\mathrm{e}^{-i\theta}) = (\mathrm{e}^{i(k+1)\theta}-\mathrm{e}^{-i(k+1)\theta}); k=0,1,2,\cdots\}$$

已构成 $L_2(S^1)$ 上的奇函数子空间的一组基底，所以 $\{\chi_k(\mathrm{e}^{i\theta})\,|\,k=0,1,2\cdots\}$ 已构成 $L_2(S^1)$ 上的偶函数子空间的一组基底. 又由于每个共轭类交 $S^1=\{\mathrm{e}^{i\theta}, 0\leqslant\theta\leqslant 2\pi\}$ 于两个点，即 $G/\widetilde{A}d = S^1/Z_2$，所以 S^1 上的偶函数恰是 $G/\widetilde{A}d$ 上的所有函数，因此 $\{\chi_k(\mathrm{e}^{i\theta})\,|\,k=0,1,2\cdots\}$ 构成 $L_2(G/\widetilde{A}d)$ 的一组正交基，则 $IR(S^3)=\{\varphi_k;\ k=0,1,2,\cdots\}$.

问题 7.3

1. 设 $\varphi_i: G\to GL(V_i)\ (i=1,2)$ 分别是 G 到 V_i 上的表示. 规定

$\varphi: G\to GL(\mathcal{L}(V_1,V_2))$ 为 $\varphi(g)\circ A = \varphi_2(g)A\varphi_1(g)^{-1}, A\in\mathcal{L}(V_1,V_2)$.

利用 $\mathcal{L}(V_1,V_2)\cong V_1\otimes V_2^*$，证明 $\varphi\cong\varphi_1\otimes\varphi_2^*$.

2. 求证：$\chi_{\varphi\oplus\psi}=\chi_\varphi+\chi_\psi, \chi_{\varphi\otimes\psi}=\chi_\varphi\circ\chi_\psi$.

3. 设 $\varphi: S^1\to S^1$ 是一个同态映射，求证：φ 必然与 φ_n 之一等价，其中 $\varphi_n: S^1\to S^1$ 定义为 $\varphi_n(\mathrm{e}^{i\theta})=\mathrm{e}^{in\theta},\quad n\in\mathbf{Z}$.

4. 设 G 是一个有限群，证明：

(1) $\dim L_2(G)=\mathrm{ord}(G)$；(2) $\dim L_2(G/\widetilde{A}d)=\mathrm{cl}(G)$.

§ 7.4 Lie 群与 Lie 代数

定义 7.4.1　设 G 是一个非空集合，满足

1) G 是一个群；

2) G 也是一个微分流形；

3) 群的运算是可微的，即由 $G \times G$ 到 G 的映射 $(g_1, g_2) \longmapsto g_1, g_2^{-1}$ 是可微映射，则称 G 是一个 Lie 群.

既然 Lie 群的结构同时含有群和微分流形的结构，我们就可以用群的可微性把群的结构线性化，这也就是 Sophus Lie 称之为"无穷小群"，而我们现在改称之为"Lie 代数"者. 在第一节中，我们将由单参数子群的研讨来实现上述线性化，确立 Lie 代数所应有的结构. 然后在第二节中将证明紧密联系 Lie 群与 Lie 代数的基本定理，说明 Lie 代数乃是 Lie 群结构的局部完全不变量.

定义 7.4.2　一个 Lie 群 G 的单参数子群就是一个由实数加法群 R（作为一个 Lie 群）到 G 中的可微同态 $\varphi: R \to G$.

我们若以 t 表示 R 中元素的参数，则 $\{\varphi(t);\ t \in \mathbf{R}\}$ 就是 G 中满足条件 $\varphi(t_1) \cdot \varphi(t_2) = \varphi(t_1 + t_2)$ 的一条可微参数曲线.

我们将以 g 表示流形 G 在单位元素 e 点的切空间. 设 $\varphi: R \to G$ 是一个 G 中的单参数子群，则它在 e 点的速度向量，亦即 $\mathrm{d}\varphi(\frac{\partial}{\partial t})$，就是 g 中的一个向量.

命题 7.4.1　对于任给向量 $X_0 \in g$，是否存在一个单参数子群 $\varphi: R \to G$，使得 X_0 恰为其在 e 点的速度向量？再者，一个单参数子群是否为其在 e 点的速度向量所唯一确定？

1) 设 $\varphi: R \to G$ 为一给定的单参数子群，则可以利用 Lie 群 G 中的右平移得到变换映射 $R \times G \to G: (t, g) \longmapsto g \cdot \varphi(t)$，它是流形 G 上的一个（单参数）可微变换群，通常叫做流动变换(flow). 再者，群的结合律也就是说任何右平移 $r_a: G \to G, r_a(g) = ga$, $g \in G (a \in G)$ 和任何左平移 $l_a: G \to G, l_a(g) = ag, g \in G (a \in G)$ 都是可换的，所以上述可微变换群的作用与任何左平移是可换的，亦即 $a(g \cdot \varphi(t)) = (a \cdot g)\varphi(t)$，因此又称之为左不变但参可微变换群，或左不变流动.

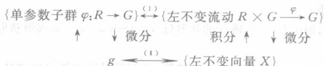
2) 设 $\varphi: R \to G$ 是一个左不变流动，则有 $\varphi(t, ag) = a\varphi(t, g)$，于是它在 G 上各点的速度向量就构成 G 上的一个左不变向量场 X，亦即 $X_{ag} = \mathrm{d}l_a(X_g)$，其中 X_{ag} 和 X_g 分别表示向量场 X 在 ag 点和 g 点的向量.

3) 设 X 是一个左不变向量场，则 X 由它在单位点的值 X_e 所唯一确定，这是因为 X_g

$= \mathrm{d}l_g(X_e)$. 反之，对应于 g 中任给向量 X_0，亦必存在一个左不变向量场 X，使得 $X_e = X_0$. 其实，我们可以用 $X_g = \mathrm{d}l_g(X_0)$ 来定义一个向量场 X，它就是那个满足 $X_e = X_0$ 的左不变向量场.

将上述分析和常微分方程组的存在唯一性定理相结合，即得下述定理：

定理 7.4.2　下列四种事物之间的自然对应都是一一映射.



证明　在上述图解中，(Ⅰ)和(Ⅱ)就是分别在分析 1) 和 3) 中所描述的自然对应，它们显然都是可逆的.

两个垂直向下的箭头都是求速度向量，所以标记以微分. 由一个左不变向量场 X 去反求一个左不变流动 $\varphi: R \to G$，使得它的速度向量场恰为 X(所依赖的，就是通常的常微分方程组的存在性和唯一性定理). 这也就建立了{左不变向量场} $\xrightarrow{\text{积分}}$ {左不变流动}这个对应.

最后，我们用 $g \xrightarrow{(\mathrm{II})}$ {左不变向量场} $\xrightarrow{\text{积分}}$ {左不变流动} $\xrightarrow{(\mathrm{I})}$ {单参数子群}的组合来达成 $g \longrightarrow$ {单参数子群}，它显然是{单参数子群} $\xrightarrow{\text{微分}} g$ 的逆映射.

基于上述定理，我们就可以用定理中建立起来的自然对应把这四种事物对等起来，即 $g \cong$ {左不变向量场} $\cong$ {左不变流动} $\cong$ {单参数子群}.

以后我们将以 g 表示这个一身具有上述四种"身份"的事物，称之为 Lie 群 G 的 Lie 代数(Lie algebra)，它就是 Lie 群 G 线性化所得的"数理结构". 现在让我们再来分析一下它究竟具有哪些自然的结构：

分析

1) 采取 g 是 G 在 θ 点的切向量空间这个身份，我们就可以赋予 g 以向量空间的结构. 若以 φ_X 表示那个以 $X \in g$ 为"初速"向量的单参数子群，则不难看出：

$$\varphi_{\lambda X}(t) = \varphi_X(\lambda t), \lambda, t \in \mathbf{R}, X \in g. \text{因此 } \varphi_X(\lambda) = \varphi_{\lambda X}(1).$$

上述分析说明可把所有 G 的单参数子群组成一个总的映射如下：

定义 7.4.3　令 $\mathrm{Exp}: g \to G, \mathrm{Exp}(X) = \varphi_X(1), X \in g$, Exp 叫做由 g 到 G 的指数映射.

指数映射的特征性质是：对任给 $X \in g$，映射

$$\mathrm{Exp}_x: R \to G, \mathrm{Exp}_x(t) = \mathrm{Exp}(tX)$$

就是上述的单参数子群 φ_X，亦即 $\varphi_X(t) = \mathrm{Exp}(tX)$ 恒成立.

从群的观点来看，g 的向量空间结构反映了 Lie 群 G 的乘法运算的一阶逼近. 也就是说，可以证明：当 s,t 都是一阶无穷小时，

$$\mathrm{Exp}(sX)\cdot\mathrm{Exp}(tY)=\mathrm{Exp}(sX+tY)$$

在略去高于一阶的无穷小后成立.

2) 采取 g 是左不变向量场的身份，我们还可以在 g 上定义一个双线性的运算[,]如下：

令 f,f_1,f_2 是定义在 G 上的任意的可微函数，X,Y 是任意两个向量场，定义 $Xf:G\to R$，$Xf(g)=X_g f$，其中 $X_g f$ 表示函数 f 在 g 点对于切向量 X_g 的方向导数. 不难验证上述运算满足下列"求导"性质：

$$X(f_1\cdot f_2)=(X f_1)\cdot f_2+f_1(X f_2).$$

反之，任何满足上述性质的运算 D 一定是关于某一个向量场的上述"求导"运算，即：设 D 为任何对 G 上所有的可微函数 f 都有定义的一个运算，而且具有上式所表示的性质，则必有唯一的一个向量场 X，使得 $Df=Xf$ 对所有的 f 都成立.

令 $[X,Y]f=X(Yf)-Y(Xf)$，则有

$$\begin{aligned}[X,Y](f_1\cdot f_2)&=X((Yf_1)\cdot f_2+f_1(Yf_2))-Y((Xf_1)\cdot f_2+f_1(Xf_2))\\&=([X,Y]f_1)f_2+f_1([X,Y]f_2).\end{aligned}$$

上式说明 $[X,Y]$ 也是一个向量场，它由 X 组合而得. 再者，当 X,Y 都是左不变时，不难验算 $[X,Y]$ 也是左不变的，这样就赋予 g 一个运算

$$[,]:g\times g\to g,$$

称之为"括积". "括积"具有下列性质：

$$(*)\begin{cases}\text{(i) 双线性：}\\ [\lambda_1X_1+\lambda_2X_2,Y]=\lambda_1[X_1,Y]+\lambda_2[X_2,Y],\\ [X,\mu_1Y_1+\mu_2Y_2]=\mu_1[X,Y_1]+\mu_2[X,Y_2].\\ \text{(ii) 斜对称性：}[X,Y]=-[Y,X].\\ \text{(iii) Jacobi 恒等式：}\\ [X,[Y,Z]]+[Y,[Z,X]]+[Z,[X,Y]]=0.\end{cases}$$

性质(i)和(ii)可以由定义推出，性质(iii)则是上式和结合律的推论.

3) 从群的观点来看，括积就是 Lie 群 G 的"不可换性"的线性化. 而上述 Jacobi 恒等式则是群的运算之结合律的线性化形式.

用无穷小的术语来说，就是当 s,t 都是一阶无穷小时，

$$\mathrm{Exp}(sX)\mathrm{Exp}(tY)\cdot\mathrm{Exp}(-sX)\mathrm{Exp}(-tY)=\mathrm{Exp}(s[X,Y])$$

在略去高于二阶的高级无穷小后成立. 换言之，$[X,Y]$ 就是度量 $\mathrm{Exp}(sX)$ 和 $\mathrm{Exp}(tY)$ 之间不可交换性的主导项，它是一个二阶的量.

通过对单参数子群的探讨来达成 Lie 群结构的线性化，所得的结构是一个具有（*）式中性质(i)，(ii) 和(iii) 的括积的向量空间 g，叫做 Lie 群 G 的 Lie 代数（当年，Sophus Lie 把它叫做无穷小群）. 还可以自然地定义由 g 到 G 的指数映射 $\mathrm{Exp}: g \to G$，其特征性质是由等式

$$\varphi_X(t) = \mathrm{Exp}(tX) \quad (t \in \mathbf{R}, X \in g)$$

所定义的映射 $\varphi_X: R \to G$，X 为"初速"向量的单参数子群. 而 g 和 G 的结构关系可以用下列两个式子说明：

$$\begin{cases} \mathrm{Exp}(sX) \cdot \mathrm{Exp}(tY) = \mathrm{Exp}(sX + tY) \text{（准确到一阶）}, \\ \mathrm{Exp}(sX)\mathrm{Exp}(tY)\mathrm{Exp}(-sX)\mathrm{Exp}(-tY) \\ \qquad = \mathrm{Exp}(st[X,Y]) \text{（准确到二阶）}. \end{cases}$$

现在我们举几个 Lie 群的实例，来看一看它们的 Lie 代数和指数映射.

例 7.4.1　设 V 是一个复（实）向量空间，V 的全线性群 $GL(V)$ 是一个 Lie 群. 事实上，由于 $GL(V)$ 是 $\mathcal{L}(V,V) \cong C^{n^2}(R^{n^2})$ 中的开集，所以它具有自然的流形结构.

另一方面，视 $GL(V)$ 为可逆矩阵组成的群，则它的乘法和求逆运算的可微性则是显然的. $GL(V)$ 在 θ 点的切空间，以 $gl(V)$ 记之. 显然 $gl(V)$ 可以和向量空间 $\mathcal{L}(V,V)$ 对等起来.

令 $A \in \mathcal{L}(V,V)$ 是 V 上一个任给的线性变换. 我们可以用下述指数级数来定义 $\mathrm{Exp}A$，即

$$\mathrm{Exp}A = I + A + \frac{1}{2!}A^2 + \cdots + \frac{1}{k!}A^k + \cdots$$

不难验证，此式中的级数总是收敛的，而且当 $AB = BA$ 时，

$$(\mathrm{Exp}A)(\mathrm{Exp}B) = \mathrm{Exp}(A + B).$$

此式的一个特殊情形是 $(\mathrm{Exp}t_1A)(\mathrm{Exp}t_2A) = \mathrm{Exp}((t_1 + t_2)A)$.

换句话说，$t \longmapsto (\mathrm{Exp}tA)$ 就定义了一个单参数子群 $R \to G$，而且可求 t 的微分，再以 $t = 0$ 代入即得

$$\frac{\mathrm{d}}{\mathrm{d}t}(\mathrm{Exp}tA)\big|_{t=0} = A.$$

这说明 $\mathrm{Exp}(tA) = \varphi_A(t)$. 所以 $GL(V)$ 的 Lie 代数应该就是 $gl(V) \cong \mathcal{L}(V,V)$，而且由指数级数所定义的映射也正好就是前面所说的从 Lie 代数到 Lie 群的指数映射（其实，这也就是指数映射这个名称的源起）. 不难验证

$$\mathrm{Exp}(sA)\mathrm{Exp}(tB) \cdot \mathrm{Exp}(-sA)\mathrm{Exp}(-tB) = \mathrm{Exp}(st(AB - BA))$$

在略去含有 s，t 的二次以上无穷小项之后成立. 这也就说明了 $gl(V)$ 上的括积应该是 $[A,B] = AB - BA$，其中 AB，BA 表示 $\mathcal{L}(V,V)$ 中的组合积.

例 7.4.2　令 $\det(A)$ 表示 A 的行列式，则

$$\det : GL(V) \to C^*(R^*)$$

是 $GL(V)$ 到非零复(实)数的乘法群的一个满同态. 所以

$$sl(V) = \{A \in GL(V); \det(A) = 1\}$$

构成 $GL(V)$ 的一个正规闭子群. 以后我们将证明,在这种情形下, $SL(V)$ 本身也是一个 Lie 群,称之为 V 上的特殊线性群. 从下述命题不难看出 $SL(V)$ 的 Lie 代数应该就是:

$$SL(V) = \{ A \in gl(V) = \mathcal{L}(V,V); \mathrm{Tr}A = 0).$$

定理 7.4.3　对于任给的 $A \in \mathcal{L}(V,V)$,恒有 $\det(\mathrm{Exp}A) = e^{\mathrm{Tr}A}$.

证明　因为 V 是实向量空间的情形可以经由复化而归于复向量空间的情形来讨论,我们不妨假设 V 是复向量空间. 设 A 为一任给线性变换,一个熟知的事实是在 V 中必存在一组基底 $\{e_1,\cdots,e_n\}$,使得 A 的相应矩阵为一个上三角矩阵(亦即子空间 $\mathrm{span}\{e_1,\cdots,e_i\}(i=1,\cdots,n)$ 都是在 A 的作用之下不变的).

$$A = \begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_n \end{pmatrix}.$$

因此,

$$A^k = \begin{pmatrix} \lambda_1^k & & & * \\ & \lambda_2^k & & \\ & & \ddots & \\ & & & \lambda_n^k \end{pmatrix}, k = 0,1,2,\cdots$$

用上述 $A^k(k=0,1,2,\cdots)$ 的矩阵形式,就可以算得

$$\det(\mathrm{Exp}A) = \det \begin{pmatrix} e^{\lambda_1} & & & \\ & e^{\lambda_2} & & \\ & & \ddots & \\ & & & e^{\lambda_n} \end{pmatrix} = \prod_{j=1}^{n} e^{\lambda_j} = \exp\Big\{\sum_{j=1}^{n}\lambda_j\Big\} = e^{\mathrm{Tr}A}.$$

例 7.4.3　我们将以 $GL(n,C)$ 表示由所有 $\det \neq 0$ 的 n 阶复方阵所组成的群,以 $GL(n,R)$ 表示由所有 $\det \neq 0$ 的 n 阶实方阵组成的群. 相对于 V 的一组基底 $\{e_1,\cdots,e_n\}$ 就有一个群的同构关系

$$GL(V) \cong \begin{cases} GL(n,C), & V \text{ 是 } n \text{ 维复空间;} \\ GL(n,R), & V \text{ 是 } n \text{ 维实空间.} \end{cases}$$

$GL(n,C)$ 和 $GL(n,R)$ 上的流形结构和群运算可微性是显然的. 因此,严格地说 $GL(V)$ 上的流形结构是从 $GL(n,C)$ 或 $GL(n,RC)$ 上借助上述同构"搬"过来的.

定义 7.4.4　Lie 群 G 和 G' 称为是同构的,若存在映射 $\varphi: G_1 \to G_2$ 使得

1)φ是群 G 到 G' 上的同构映射；

2)φ是流形 G 到 G' 上的微分同胚(diffeomerphism)，映射 φ叫做 G 到 G' 上的(Lie 群的)同构映射.

由此定义可知，上面的同构是 Lie 群的同构.

定义 7.4.5 设 g 和 g' 分别是 Lie 群 G 和 G' 的 Lie 代数，若存在一个映射 $\rho: g' \to g'$，满足下列条件

1)ρ 是向量空间 g' 到 g' 上的同构映射；

2)$[\rho X, \rho Y] = \rho[X, Y], \forall X, Y \in g'$，

我们说 g' 与 g' 是同构的，ρ 叫做 Lie 代数 g' 到 g' 上的同构映射. 由矩阵的指数级数知，$GL(n,C)$ 和 $GL(n,R)$ 的 Lie 代数分别是 $M(n,C)$ 和 $M(n,R)$，$M(n,C)$ 和 $M(n,R)$ 分别是 n 阶复(实)方阵全体构成的集合. 而且显然有 Lie 代数的同构关系

$$gl(V) \cong \mathcal{L}(V,V) \cong \begin{cases} M(n,C); \\ M(n,R). \end{cases}$$

例 7.4.4 我们以 $SL(n,C)$ 和 $SL(n,R)$ 分别表示由行列式为 1 的复(实)方阵所构成的 Lie 群(叫做特殊线性群)，$sl(n,C)$ 和 $sl(n,R)$ 分别表示它们的 Lie 代数. 不难看出，$sl(n,C)$ 和 $sl(n,R)$ 分别由迹为零的复(实)方阵所组成，而且存在同构关系：

$$SL(V) \cong \begin{cases} SL(n,C); \\ SL(n,R). \end{cases} \quad \text{及} \quad sl(V) \cong \begin{cases} sl(n,C); \\ sl(n,R). \end{cases}$$

由例 7.4.3 和例 7.4.4，我们对上述两组群 $GL(V)$ 与 $GL(n,C)$(或 $GL(n,R)$)及其 Lie 代数将不加区别，对 $SL(V)$ 及 $SL(n,C)$(或 $SL(n,R)$)也不加区别.

例 7.4.5 设 V 是一个 m 维复向量空间，$<,>$ 是定义在 V 上的非退化双线性型. 若对任何的 $x, y \in V$，$<x,y> = <y,x>$ 恒成立，称之为对称的，若 $<x,y> = -<y,x>$ 恒成立，则称之为反对称或斜对称的.

设 $<,>$ 是 VV 上一个任意给定的对称的或反对称的非退化双线性型，容易验证：$GL(V)$ 中所有令 $<,>$ 不变的元素 g(亦即 $<gx,gy> = <x,y>$ 对任何 $x,y \in V$ 恒成立)，组成一个闭子群，因此它本身也是一个 Lie 群.

当 $<,>$ 是对称的时，这个子群称为复正交群，记为 $O(V)$. 类似于例 7.4.1 的讨论，我们也可以讨论相应的矩阵群. 由线性代数的知识可知，V 中存在一组基 $e_1, \cdots, e_m$，使得 $<e_i, e_j> = \delta_{ij}(1 \leqslant i, j \leqslant m)$，称之为标准正交基. 任取 $g \in O(V)$，g 在上述基下的矩阵仍记为 g，则容易验证：

$$g \in O(V) \Leftrightarrow g^T \circ g = g \circ g^T = I_m \quad (g^T \text{ 表示 } g \text{ 的转置}).$$

满足上式的复矩阵称为复正交阵. 我们把 $GL(m,C)$ 中所有复正交矩阵组成的子群记为 $O(m,C)$，则 $O(V) \cong O(m,C)$.

现在我们来讨论复正交群的 Lie 代数，记之为 $o(n,C)$.

任取 $X \in o(n,C)$，有 $\mathrm{Expt}X \in O(n,C)$，$t \in \mathbf{R}$. 因此对于任何 $u,v \in V$，

$$< \mathrm{Expt}X \cdot u, \mathrm{Expt}X \cdot v > = < u,v >.$$

对上式两边分别在 $t=0$ 处求导，我们立刻得出 $< Xu,v > + < u,Xv > = 0$.

此式表明，X 在标准正交基下的矩阵（仍记为 X）是一个斜对称矩阵；反过来也是对的. 因此，$X \in o(n,C) \Leftrightarrow X$ 是斜对称的.

如果我们以上述标准正交基为基底来造一个实数域上的向量空间 V'，则 V' 是一个欧氏空间. $GL(V')$ 中令 $<,>$ 不变的元素全体组成 $GL(m,R)$ 的一个闭子群，称为实正交群，简称为正交群，记为 $O(m)$.

不难证明它是一个紧 Lie 群，且有

$$g \in O(m) \Leftrightarrow g^T \circ g = g \circ g^T = I_m, \quad g \in GL(m,R)$$

若 $<,>$ 是反对称的，由 $GL(V)$ 中令 $<,>$ 不变的元素组成的子群叫做复辛群，记为 $Sp(V)$. 由线性代数知识可知，$\dim V$ 一定是偶数. 设 $m=2n$，则在 V 中存在一组基 $e_1, \cdots, e_m$，满足

$$\begin{cases} < e_i, e_{n+i} > = - < e_{n+i}, e_i > = 1 & (i = 1, \cdots, n), \\ < e_k, e_l > = 0, & 若\ k,l\ 不满足上述条件. \end{cases}$$

如果我们仍把 $GL(V)$ 中元素 g 在上述基下的矩阵记为 g，则不难验证：

$$g \in Sp(V) \Leftrightarrow g^T J_n g = J_n,$$

其中

$$J_n = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}.$$

令 $Sp(n,C) = \{g \in GL(m,C); g^T J_n g = J_n (m = 2n)\}$，则 $Sp(V)$ 与 $Sp(n,C)$ 之间存在自然同构，今后对这两个群也不加区别，均称为复辛群.

现在讨论复辛群的 Lie 代数 $Sp(n,C)$. 任取 $X \in sp(n,C)$，令 $g = \mathrm{Expt}X (t \in \mathbf{R})$. 注意到 $A\mathrm{Exp}XA^{-1} = \mathrm{Exp}(AXA^{-1})$ 以及 $(\mathrm{Exp}X)^T = \mathrm{Exp}X^T$，因此有

$$g^T J_n g = \mathrm{Exp}(tX)^T J_n \mathrm{Expt}X = J_n，或者\ J_n{}^{-1} \mathrm{Exp}(tX)^T J_n = \mathrm{Expt}(-X).$$

即 $\mathrm{Expt}(J_n{}^{-1} X^T J_n) = \mathrm{Expt}(-X)$. 所以，我们得知 $X \in sp(n,C) \Leftrightarrow X^T J_n + J_n X^T = 0$.

将 X 写成分块形式：

$$X = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

则条件 $X \in sp(n,C) \Leftrightarrow X^T J_n + J_n X^T = 0$ 等价于

$$X = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix} \in sp(n,C) \Leftrightarrow \begin{cases} X_2 = X_2^T, X_3 = X_3^T, \\ X_1^T + X_4 = 0. \end{cases}$$

所以

$$sp(n,C)=\left\{\begin{pmatrix} X_1 & X_2 \\ X_3 & -X_1^T \end{pmatrix};\ \begin{matrix} X_i(i=1,2,3)\text{ 是 } n\times n \text{ 复矩阵,} \\ X_2,X_3 \text{ 是对称的} \end{matrix}\right\}.$$

例 7.4.6 设 V 是一个 n 维酉空间,$(,)$ 是其上定义的正定 Hermite 型(也称为酉积),则 $GL(V)$ 中所有令$(,)$不变的元素全体组成它的一个闭子群,称为酉群,记为 $U(n)$. 容易看出,$U(n)$ 也是一个紧群.

现在讨论与之相应的矩阵群. 众所周知,在 V 中存在标准正交基(或称为酉基)$e_1,\cdots,e_n$,我们也将 $g\in GL(V)$ 与它在此基下的矩阵用同一记号 g 表示,则容易验证:

$$g\in U(n)\Leftrightarrow g^T\circ g=g\circ g^T=I_n.$$

换句话说,$g\in U(n)$ 当且仅当 g 是一个酉矩阵. 因此,所有 n 阶酉矩阵组成的 Lie 群与 $U(n)$ 同构,今后也不加区别,通记为 $U(n)$.

上述这些 Lie 群,在 Lie 群理论中占有非常重要的地位,它们是 Lie 群的典型实例,应用十分广泛,一般统称为典型群.

我们指出,Lie 代数本身也是一种具有独立研究价值的数理模型. 我们可以独立于 Lie 群,给出下列抽象 Lie 代数的定义.

定义 7.4.6 设 g 是一个实(复)向量空间,在 g 上定义一种新的运算$[,]:g\times g\to g$,称之为括积,满足($*$)式中条件 1),2) 和 3). 这样一个代数体系,我们称之为实(复)数域上的(抽象)Lie 代数.

进一步推广之,还可以研究一般域上的 Lie 代数. 抽象 Lie 代数的研讨是近世代数学中一个蓬勃开展的领域,而且还和许多其他领域密切相关.

§7.5 Lie 群的对称性

在上一节中,我们通过对单参数子群的探讨,运用常微分方程组解的存在唯一性定理来达成了 Lie 群结构的线性化,从而对于每一个 Lie 群 G,作出了它的 Lie 代数 g,它是一种具有($*$)式中性质 1),2) 和 3) 的括积的线性空间.

设 $h:G_1\to G_2$ 是一个由 G_1 到 G_2 的可微同态映射. g_1,g_2 分别是 G_1 和 G_2 的 Lie 代数,眼下我们可以采用它们是单参数子群的身份来考虑. 对于任给 $X\in g_1$,$\varphi_X:R\to G_1$ 是 G_1 相应的单参数子群,则显然

$$h\circ\varphi_X:R\to G_1\to G_2$$

是 G_2 中的一个单参数子群,所以唯一存在一个 $h(X)\in g_2$,使得

$$(h\circ\varphi_X)(t)=\varphi_{\dot h(X)}(t).$$

改用指数映射的符号来写就是:存在一个由 h 诱导出来的 Lie 代数同态(即保持括

积不变的向量空间的同态) $\widetilde{h}: g_1 \to g_2$，使得如图 7.7 所示图解是可换的. 其中 $h\mathrm{Exp}(tX) = \mathrm{Exp}(t \circ \widetilde{h}(X))$. 上面的结果说明 $\widetilde{h}$ 也就是 h 的线性化，总之线性化的过程就好像给所有的 Lie 群和 Lie 群之间的各种可微同态所组成的范畴(category)照了一张集体照. 一个 Lie 群 G 的像就是它的 Lie 代数 g，而一个可微同态 $h: G_1 \to G_2$ 的像就是它所诱导而得的 Lie 代数同态 $\widetilde{h}: g_1 \to g_2$，则 Lie 代数及其同态这个范畴在本质上远比 Lie 群及其同态那个范畴更为初等.

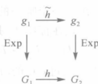


图 7.7

定义 7.5.1　设 G 是 Lie 群，它的一个子流形 H 称为是 G 的 Lie 子群，若

1) H 是一个(抽象)子群，

2) H 本身是一个拓扑群.

设 H 是 G 的 Lie 子群，它自然是一个 Lie 群. 设 η 是 H 的 Lie 代数，则不难证明 η 是 g 的 Lie 子代数(亦即在括积之下封闭的线性子空间，$[\eta, \eta] \subset \eta$). 在上一节我们研讨的基本问题就是单参数子群的存在性和唯一性. 很自然地，我们现在所要研讨的基本问题就是下面所述的 Lie 子群的存在性和唯一性问题：

对于 g 中的任给 Lie 子代数 η，是否一定存在一个连通 Lie 子群 H，以 η 为其 Lie 代数？这样的连通 Lie 子群是否唯一？

上述问题的答案又是肯定的，这就是 Sophus Lie 在 Lie 群论中首先建立起来的基本定理.

定理 7.5.1(基本定理)　设 G 是一个 Lie 群，对于 G 的 Lie 代数 g 的任何一个 Lie 代数 η，存在唯一的一个 G 的连通 Lie 子群 H，使得如图 7.8 所示图解是可交换的.

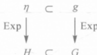


图 7.8

证明　设 $X_1, X_2, \cdots, X_m$ 是向量子空间 η 的任取的一组基底，我们现在采用它们是 G 上的左不变向量场这种身份，则它们在 G 的每一点 g 的切空间中张成一个子空间，亦即 $\mathscr{D}(g) = \mathrm{span}\{X_1(g), \cdots, X_m(g)\}$，其中 $X_i(g)$ 表示向量场 X_i 在 g 点的值. 这种在每点的切空间中取定一个 m 维子空间叫做 G 上的一个 m 维分布，本质上它可以说是向量场的高维推广. 因为 $X_i (1 \leqslant i \leqslant m)$ 都是左不变的，即 $\mathrm{d}l_a(X_i(g)) = X_i(ag)$，所以由它们所张成的分布 $\mathscr{D}$ 也是左不变的，即 $\mathrm{d}l_a(\mathscr{D}(g)) = \mathscr{D}(ag)$. 再有，因为 $\eta = \mathrm{span}\{X_1, X_2, \cdots, X_m\}$ 是个 Lie 子代数，所以 $[X_i, X_j] (1 \leqslant i, j \leqslant m)$ 总是可以用 $X_1, \cdots, X_m$ 的适当线性组合加以表达. 这就说明了上述分布 $\mathscr{D}$ 满足 Frobenius 定理中的可积条件. 所以

存在着一个唯一的相应于 $\mathscr{D}$ 的极大积分子流形，通过单位元素 e，以表之.

现在证明 H 是一个连通子群. 设 h 是 H 中的任意元素. 因为 $\mathscr{D}$ 是左不变的，所以 $l_{h^{-1}} \cdot H = h^{-1} \cdot H$ 当然也是 $\mathscr{D}$ 的一个极大积分子流形. 由定义，$e \in h^{-1} \cdot H$，即 $h^{-1} \cdot H$ 也是过 e 点的. 由极大积分子流形的唯一性即得 $h^{-1} \cdot H = H$. 但是 h 是任意的，所以 $H^{-1} \cdot H = \bigcup h^{-1} \cdot H = H$. 这也就证明了 H 是一个连通子群.

推论 7.5.2　设 G_1 是一个单连通 Lie 群，G_2 是一个连通 Lie 群. g_1, g_2 分别是 G_1 和 G_2 的 Lie 代数，则对于任给的 Lie 代数同态 $\widetilde{h}: g_1 \to g_2$，存在一个唯一的 Lie 群同态 $h: G_1 \to G_2$，使得如图 7.9 所示图解可换.

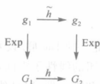


图 7.9

证明　要把上述关于同态的问题归于已解答的子群的情形，常用的手法是把“映射”转换为它的图像(graph)，其具体做法如下：令

$$\Gamma(\widetilde{h}) = \{X_1, \widetilde{h}(X_1); X_1 \in g_1\} \subset g_1 \times g_2,$$

则 $\Gamma(\widetilde{h})$ 是 $g_1 \times g_2$ 的 Lie 子代数. 而 $g_1 \times g_2$ 显然就是 $G_1 \times G_2$ 的 Lie 代数，所以由基本定理可知，在 $G_1 \times G_2$ 中存在一个唯一的连通 Lie 子群 K，使得如图 7.10 所示图解可换.

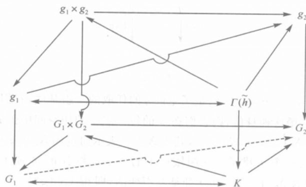


图 7.10

在上述图解中，所有垂直向下的映射都是 Exp. 再者，因为 $\Gamma(\widetilde{h}) \to g_1$ 是一个 Lie 代

数的同构，所以相应的映射 $K \to G_1$ 是一个覆盖同态. 但 G_1 是单连通的，因此这个由 K 到 G_1 上的同态必须是同构，它的逆映射自然是由 G_1 到 K 上的同构. 把它与 K 到 G_2 的同态映射组合，便得出所求之由 G_1 到 G_2 的同态 h，它与 $\widetilde{h}$ 可换是显然的.

利用基本定理，我们还可以证明下列重要定理.

定理 7.5.3　设 G 是 Lie 群，H 是 G 的一个(抽象)子群. 假设 H 是 G 的一个闭子集，则在 H 上存在唯一的可微结构，使得 H 是 G 的一个拓扑 Lie 子群.

证明　设 g 是 G 的 Lie 代数. 令 $\eta = \{X \in g; \mathrm{Exp}tX \in H, 对所有\ t \in \boldsymbol{R}\}$.

由于 η 是 g 的 Lie 子代数(这里要用到闭性). 由基本定理，G 中有一个连通子群 H^*，它的 Lie 代数是 η. 显然 $H^* \subset H$. 进一步可以证明，若 H 取 G 的相对拓扑，且记 H 的单位元连通分支为 H_0，则作为拓扑群，$H^* = H_0$. 得证.

1) 对任给连通 Lie 群 G，都存在唯一的一个单连通覆盖群 $\widetilde{G} \to G$. 上述覆盖同态的核是 $\widetilde{G}$ 中的一个离散正规子群，它必定包含在 $\widetilde{G}$ 的中心之中.

2)Ado 定理证明了任何抽象 Lie 代数都可以与某个 $gl(n,\boldsymbol{C})$ 的一个适当的 Lie 子代数同构. 由此可见抽象 Lie 代数都可以实现为一个 Lie 群的 Lie 代数.

推论 7.5.4　所有有限维 Lie 代数及其同态和所有单连通 Lie 群及其同态之间的一一在上的对应.

最后我们举两个有关覆盖同态的例子.

例 7.5.1　$(\boldsymbol{R}^1, +)$ 和 $(S^1, \cdot)$ 都是一维可换连通 Lie 群. 它们的 Lie 代数显然是同构的. 存在很多由 $\boldsymbol{R}^1$ 到 S^1 的覆盖同态，如 $t \longmapsto e^{2\pi int}, n \in \boldsymbol{Z}$. 但是 S^1 到 $\boldsymbol{R}^1$ 的唯一同态是把所有元素都映射到零者. 上述现象的基本原因是：$\boldsymbol{R}^1$ 是单连通的，但 S^1 则不是单连通的.

例 7.5.2　我们已知 S^3 的伴随表示就是 $S^3 \to SO(3) \cong S^3/\{\pm 1\}$，即把 $q \in S^3$ 映射到由 $X \longmapsto q \times q^{-1} (X \in \mathbf{Q} \cong \boldsymbol{R}^4)$ 在与实轴垂直的 $\boldsymbol{R}^3$ 上所诱导的正交变换，这也就是说 $S^3 \to SO(3)$ 是 $SO(3)$ 的覆盖群. 所以它们的 Lie 代数是同构的. 但是不存在 $SO(3)$ 到 S^3 的非平凡同态. 其基本原因也在于 S^3 是单连通的，而 $\pi_1(SO(3)) \cong \boldsymbol{Z}_2$.

问题 7.5

1. 设 $H \in G$ 是 G 的一个 Lie 子群，g, η 分别是 G 和 H 的 Lie 代数，求证：η 是 g 的 Lie 子代数.

2. 利用指数映射证明每一个 Lie 群 G 都有一个单位元 e 点的邻域，它不包含任何不等于 $\{e\}$ 的子群.

3. 证明由 $SO(3)$ 到 S^3 的同态是平凡的.

4. 设 G 是 $GL(4,\boldsymbol{R})$ 中下列元素组成的 Lie 子群：

$$\begin{pmatrix} \cos\gamma & \sin\gamma & 0 & \alpha \\ -\sin\gamma & \cos\gamma & 0 & \beta \\ 0 & 0 & 1 & \gamma \\ 0 & 0 & 0 & 1 \end{pmatrix} (\alpha,\beta,\gamma \in \mathbf{R}),$$

求它的 Lie 代数 $\eta \subset g^1(4,\mathbf{R})$.

5. 在矩阵群中,还有几种十分重要的群,

$$SU(n) = U(n) \cap SL(n,\mathbf{C}),$$
$$SO(n) = O(n) \cap SL(n,\mathbf{R}),$$
$$Sp(n) = Sp(n,\mathbf{C}) \cap U(2n).$$

验证它们都是紧致连通 Lie 群,并求出它们的 Lie 代数.

§7.6　伴随变换与伴随表示

一个可交换的群,它的结构是相当简单的. 例如,所有有限生成的可交换群具有十分简单的结构定理. 任何连通可换 Lie 群都是向量加群除以一个部分格点子群的商群. 因此,群论的重点在于群的"不可交换性"的研讨. 什么是一个群 G 的不可交换性呢?一个直截了当的提法就是:一个群 G 的不可交换性就是下述伴随变换:

定义 7.6.1　G 是一个群,将群 G 表示成作用在其本身上的共轭(内)自同构群的这个变换称为伴随变换

$$\widetilde{A}d: G \times G \to G, (g,\ x) \to gxg^{-1}.$$

如果上述变换群是平凡变换群的情形就说明 G 是交换群. 如果 G 是一个 Lie 群,则其伴随变换就是一个可微变换群,它的几何结构可以说是整个 Lie 群论的枢纽.

伴随变换 $\widetilde{A}d: G \times G \to G$ 把每一个 $g \in G$ 表示成一个 G 本身的(内)自同构

$$\sigma_g: G \to G, \sigma_g(x) = gxg^{-1}.$$

相应地就有它在 Lie 代数 g 上所诱导而得的自同构

$$Ad(g): g \to g,$$

即图 7.11 是可换的.

$$g(\mathrm{Exp}tX)g^{-1}: \mathrm{Exp}(tAd(g)X), X \in G, t \in \mathbf{R}.$$

让上述 g 在 G 中变动,就得到一个同态

$$Ad: G \to GL(g),$$

叫做 G 的伴随表示. 再者,上述同态又进而诱导出下述的 Lie 代数同态:

$$ad: g \to gl(g),$$

$$\begin{array}{ccc} g & \xrightarrow{Ad(g)} & g \\ \downarrow \text{Exp} & & \downarrow \text{Exp} \\ G & \xrightarrow{\sigma_g} & G \end{array}$$

图 7.11

$$\begin{array}{ccc} g & \xrightarrow{ad} & gl(g) \\ \downarrow \text{Exp} & & \downarrow \text{Exp} \\ G & \xrightarrow{Ad} & GL(g) \end{array}$$

图 7.12

使得图 7.12 可交换.

亦即

$$Ad(\text{Exp}sY) = \text{Exp}(s \cdot adY), Y \in g, s \in \mathbf{R}.$$

在本质上,上面所做的就是对于伴随变换映射 $\widetilde{A}d(g,x) = gxg^{-1}$ 这个"二变数"映射进行逐步线性化. 换句话说,先把 x 代以 $\text{Exp}tX$,就可以把 x 这个"变数"线性化而得

$$g(\text{Exp}tX)g^{-1} = \text{Exp}(tAd(g)X).$$

第二步再把 g 代以 $\text{Exp}(sY)$,这样就可以把 g 这个"变数"也线性化了,即得

$$\begin{aligned} &\text{Exp}(sY) \cdot \text{Exp}(tX) \cdot \text{Exp}(-sY) = \text{Exp}(t \cdot Ad(\text{Exp}sY)X) \\ &\quad = \text{Exp}(t\text{Exp}(s \cdot adY)X) = \text{Exp}(tX + ts(ad(Y)X) + \text{高阶项}). \end{aligned}$$

可以得出

$$\text{Exp}(sY)\text{Exp}(tX)\text{Exp}(-sY)\text{Exp}(-tX) = \text{Exp}(tsad(Y)X).$$

但是在前面已知

$$\text{Exp}(sY)\text{Exp}(tX)\text{Exp}(-sY)\text{Exp}(-tX) = \text{Exp}(ts[Y,X]),$$

这就证明了下述定理:

定理 7.6.1　$ad(Y) \cdot X = [Y, X]$.

先以 $GL(V)$ 为例来看看它的伴随表示是什么?由于 $GL(V)$ 的 Lie 代数就是 $gl(V) \cong \mathcal{L}(V,V)$,而其指数映射可以用幂级数直接写出,即:

$$\text{Exp}X = I + X + \frac{1}{2!}X^2 + \cdots + \frac{1}{k!}X^k + \cdots, \quad X \in \mathcal{L}(V,V).$$

由此式不难看出,对于任给 $A \in \mathcal{L}(V,V), X \in gl(V) = \mathcal{L}(V,V)$,恒有

$$\begin{aligned} A\,\text{Exp}tXA^{-1} &= A(I + tX + \frac{t^2}{2!}X^2 + \cdots + \frac{t^k}{k!}X^k + \cdots)A^{-1} \\ &= I + t(AXA^{-1}) + \frac{t^2}{2!}(AXA^{-1})^2 + \cdots + \frac{t^k}{k!}(AXA^{-1})^k + \cdots \\ &= \text{Exp}t(AXA^{-1}). \end{aligned}$$

由此得:$Ad(A)X = AXA^{-1}$.

由于 $GL(V) \cong GL(n,\boldsymbol{C})$(或 $GL(n,\boldsymbol{R})$),$gl(V) \cong M(n,\boldsymbol{C})$(或 $\boldsymbol{M}(n,\boldsymbol{R})$),所以我们可以把上述结果改写为 $GL(n,\boldsymbol{C})$ 和 $GL(n,\boldsymbol{R})$ 的伴随表示的应有形式.

设 H 是 G 的一个连通 Lie 子群，η 是它的 Lie 代数，则 $Ad_G: G \to GL(g)$ 和 $Ad_H: H \to GL(\eta)$ 之间有如下关系：以符号 $Ad_G|_H$ 表示线性表示

$$H \subset G \xrightarrow{Ad_G} GL(g),$$

则 η 是在 $Ad_G|_H$ 的作用下不变的子空间，把 H 的作用限制在 η 上即得 Ad_H.

根据定理 7.6.1，对 $\forall Z \in g, adZ \in gl(g)$. 由 Jacobi 恒等式知，$adZ$ 有下列性质：

$$adZ \cdot [X,Y] = [Z,[X,Y]] = [[Z,X],Y] + [X,[Z,Y]] = [adZ \cdot X, Y] + [X, adZ \cdot Y].$$

定义 7.6.2 Lie 代数 g 的一个线性变换 D 叫做 g 的导子，若

$$D[X,Y] = [DX, Y] + [X, DY], \quad \forall X,Y \in V.$$

我们用 $\partial(g)$ 表示 g 的所有导子组成的集合. $adZ(Z \in g)$ 自然是 g 的一个导子，这样的导子叫做内导子. $ad(g) \subset \partial(g)$.

令 $\mathrm{Aut}(g)$ 表示 g 的自同构群，则有

定理 7.6.2 $D \in \partial(g)$ 当且仅当 $\mathrm{Exp}tD \in \mathrm{Aut}(g)$.

证明 只要证明

$$[DX, Y] = [DX, Y] + [X, DY]$$

$$\Leftrightarrow (\mathrm{Exp}tD)[X,Y] = [\mathrm{Exp}tD \cdot X, \mathrm{Exp}tD \cdot Y]$$

即可. 由 Exp 的定义，对 $D[X,Y] = [DX, Y] + [X,DY]$ 两边对 t 在 $t = 0$ 处求导，就得出上式. 另一方面，对任何自然数 k，可验证

$$D^k[X,Y] = \sum_{i+j=k} \frac{k!}{i!j!}[D^iX, D^jY], i \geqslant 0, j \geqslant 0, \text{其中 } D^0 \text{ 表恒等映射}.$$

下面我们假设所讨论的 Lie 群都是紧致连通的而不再另外声明. 有了紧致性，就可以在 Lie 群 G 的单位元 e 点的切空间 g 上取定一个在 $Ad(G)$ 的作用下不变的内积 $<,>$，即

$$< Ad(g)X, Ad(g)Y > = < X,Y >, \quad X,Y \in g, g \in G.$$

对于这样取定的内积，我们再任取 g 的一组标准正交基 $\{X_i; 1 \leqslant i \leqslant n\}$，即 $< X_i, X_j > = \delta_{ij}$. 然后，我们再用左平移把 $\{X_i; 1 \leqslant i \leqslant n\}$ 分别扩张成 G 上左不变向量场，而且依然用符号 X_i 记之. 这样就可以唯一地在 G 上的每点的切空间上都取定内积，使得 $\{X_i(x); 1 \leqslant i \leqslant n\}$ 恰为在 x 点的切空间的标准正交基. 这也就在流形 G 上建立了一个黎曼空间的结构. 由正交向量场组 $\{X_i; 1 \leqslant i \leqslant n\}$ 的左不变性容易看出：所有左平移都是这个黎曼空间的正交变换. 再者，由于在 g 上的内积是 $Ad(G)$ 不变的，不难验证所有右平移也是它的正交变换. 令 $g(a)$ 为 G 在 a 点的切空间，$g(e) = g$. dl_a, dr_a 分别是左，右平移 l_a, r_a 在切空间之间所诱导的线性映射，则有如图 7.13 所示可换图解.

其中 $a \cdot a^{-1}xa = xa$. 因为 dl_a 和 $Ad(a^{-1})$ 都是正交的，所以 dr_a 也是正交的. 因此，

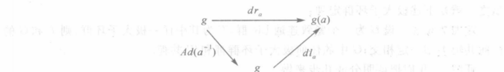


图 7.13

从本节开始，我们总是假定一个紧致连通 Lie 群 G 具有一个在左、右平移下都正交的黎曼结构而不再另加声明. 当然，伴随变换 $\widetilde{A}d: G\times G\to G$ 对于上述黎曼结构而言也是一个正交变换群，本章的主要课题就是要研讨这个正交变换群的轨道结构的几何，简称为轨几何. 一个群 G 的伴随变换的轨道就是它的共轭类，所以伴随变换的轨几何也就是共轭类的几何.

前面我们已经分析了 S^3 这个紧致 Lie 群的共轭类几何，其结果为：S^3 中的任何共轭类都和 S^1 垂直相交，而且和半圆 $\{e^{i\theta}; 0\leqslant\theta\leqslant\pi\}$ 只交于一点；再者，含有 $e^{i\theta}$ 的共轭类的面积是 $c\cdot\sin^2\theta$，其中 c 是一个常数. 上述关于共轭类几何的结果在 S^3 的所有复不可约线性表示的分类中起了决定性的作用.

现在让我们再以 $U(n)$ 为例，来看一看它的共轭类几何. 在线性代数中有一个熟知的事实：任何酉矩阵 A 在 $U(n)$ 中可以对角化，换句话说，存在适当的 $g\in U(n)$，使得 gAg^{-1} 为一个对角酉矩阵. 令

$$T^n=\left\{\begin{pmatrix} e^{i\theta_1} & & & \\ & e^{i\theta_2} & & \\ & & \ddots & \\ & & & e^{i\theta_n}\end{pmatrix}; 0\leqslant\theta_i\leqslant 2\pi\right\}\cong S^1\times\cdots\times S^1$$

为所有 n 阶对角酉阵所组成的子群，它同构于 n 个 S^1 的直积，称之为秩 n 的环群，则上述事实的另一说法是 T^n 和 $U(n)$ 中的任何共轭类都相交. 再者，设 T' 是 $U(n)$ 中的一个任给的子环群. 我们可以把 $T'\subset U(n)$ 想成一个 T' 的作用在 $\mathbf{C}^n$ 上的酉表示，$e_1,\cdots,e_n$ 是 $\mathbf{C}^n$ 相应的酉基. 因为 T' 是可换的，而任何可换群的不可约复表示都必须是一维的，所以必存在一个 $\mathbf{C}^n$ 的正交分解：

$$\mathbf{C}^n=V_1\oplus V_2\oplus\cdots\oplus V_n,$$

其中 V_i 都是复一维的 T'-不变子空间. 在每个 V_i 中各取一个单位长向量 a_i. 令 $Ae_i=a_i(i=1,\cdots,n)$，则 A 是一个酉变换，且不难看出 $A^{-1}T'A\subset T^n$，亦即 $U(n)$ 中的任意子环群都共轭于 T^n 中的一个子群，所以 T^n 当然是 $U(n)$ 中的一个极大子环群，而且 $U(n)$ 中的任意极大子环群都和 T^n 共轭.

基于上述分析，很自然就要问一问：上面这个关于 $U(n)$ 的共轭类几何和子环群的基本结果是否可以推广到所有的紧致连通 Lie 群呢？E. Cartan 在 Lie 群论方面的重要贡

献之一就是下述极大子环群定理：

定理 7.6.3　设 G 为一个紧致连通 Lie 群，T 为其中任一极大子环群，则 T 和 G 的任何共轭类都一定相交；G 中的任何极大子环群都和 T 共轭.

证明　我们把证明分成几步来做：

1）设 T 是 G 的一个极大子环群. 我们将 G 的伴随变换 $\widetilde{A}d$ 和伴随表示 $Ad: G\times g \to g$ 分别限制到 T 上，即得

$$\widetilde{A}d|_T : T\times G\to G \text{ 和 } Ad|_T : T\times g\to g.$$

则显然有：T 在 $\widetilde{A}d|_T$ 的作用下每点都固定不动，而且对于 T 上的任意一点 t，$\widetilde{A}d|_T$ 在 t 点的（G 的）切空间 $g(t)$ 上所诱导的线性表示都和 $Ad|_T : T\times g\to g$ 等价.

因为任何可换群的不可约复表示都必须是一维的，不难由此推论而得：任何环群的非平凡实不可约表示都是二维的. 所以 $Ad|_T$ 可以分解如下，即 $Ad|_T = k$ 维平凡表示 $\oplus \sum \varphi_i$.

相应地，g 就分解成不变子空间的直和 $g = R^k \oplus \sum R^2(\varphi_i)$，其中 $R^2(\varphi_i)$ 是非平凡表示 $\varphi_i : T\to SO(2)$ 的表示空间. 由 T 的可换性容易看出上述 R^k 包含 T 的 Lie 代数 η. 再由 T 的极大性就可断言 $R^k \supseteq \eta$. 要不然，就可以找到一个包含 η 而且比 η 更高维的可换 Lie 子代数，再用基本定理即得 G 中一个包含 T 而且比 T 高维的可换连通子群，它的闭包 T'，当然是一个包含 T 而且比 T 高维的子环群，这就和 T 的极大性相矛盾，所以 $R^k = \eta$. 今后称 η 为 g 的 Cartan 子代数.

2）因为 $\varphi_i : T\to SO(2)$ 都是非平凡的，所以 $\ker(\varphi_i)$ 都是 T 的低一维子群. 因此 $\bigcup_{\varphi_i}\ker(\varphi_i)\neq T$，且不含 T 中的任何非空开集. 任取 $t_0\in T\setminus \bigcup_{\varphi_i}\ker(\varphi_i)\neq T$，令 G_{t_0} 是 t_0 在 G 中的中心化子，即 $G_{t_0} = \{g\in G; gt_0g^{-1} = t_0\}$，它自然是 G 的一个子群. 用 $G^0_{t_0}$ 表示由 G_{t_0} 的单位元连通分支所组成的连通子群，g_{t_0} 是 $G^0_{t_0}$ 的 Lie 代数（注意，这里的 g_{t_0} 不表示 G 在 t_0 点的切空间，也就是说 $g_{t_0}\neq g(t_0)$）. 由中心化子的定义，显然有 $G^0_{t_0}\supset T$，我们要证明 $G^0_{t_0} = T$. 设 $X\in g_{t_0}$ 是其中任给元素，则 $\mathrm{Exp}(sX)\in G^0_{t_0}$，亦即

$$\mathrm{Exp}s(Ad(t_0)x) = t_0(\mathrm{Exp}tsX)t_0^{-1} = \mathrm{Exp}sX,\ s\in \boldsymbol{R},$$

因此，$Ad(t_0)X = X$. 由于 $t_0\in T\setminus \bigcup \ker(\varphi_i)$，这只有在 $X\in \eta(\subseteq R^k)$ 时才可能，所以 $g_{t_0} = \eta, G^0_{t_0} = T$.

3）令 $G(t_0)$ 表示过 t_0 点的 $\widetilde{A}d(G)$- 轨道，也就是包含 t_0 的共轭类. 显然，$G(t_0)\cong G/G_{t_0}$（作为流形）. 所以

$$\dim G(t_0) = \dim G\backslash G_{t_0} = \dim G - \dim T,\text{ 亦即 } \dim G(t_0) + \dim T = \dim G.$$

再有，在 $\widetilde{A}d|_T$ 的作用之下，$t_0\in T$ 是一个不动点，$G(t_0)$ 和 T 则分别是不变子流形，它们相交于 t_0 点. 因此，$\widetilde{A}d|_T$ 在定点 t_0 处关于 G 的切空间 $g(t_0)$ 上所诱导的线性表示当然也

就有两个不变线性子空间,那就是 T 在 t_0 点的切空间和 $G(t_0)$ 在 t_0 点的切空间. 再者,在 1) 中我们也已指出:可以用 dl_{t_0} 把表示(T,g) 与 $\langle T, g(t_0)\rangle$ 两者等同起来,所以有 $g(t_0)=\boldsymbol{R}^k \oplus \sum R^2(\varphi_i)$.

在上述分解式中,显然 $\boldsymbol{R}^k=\eta$ 就是那个 T 在 t_0 点的切空间,而 $\sum R^2(\varphi_i)$ 就是那个 $G(t_0)$ 在 t_0 点的切空间(因为 T 对于 $G(t_0)$ 在 t_0 点的切空间的作用不可能含有任何非零的不动向量. 不然的话,就容易推出 T 并非是极大子环群). 所以 $G(t_0)$ 和 T 在 t_0 点正交!

4) 现在我们就容易运用前述的 G 上的黎曼结构来完成本定理的证明.

先介绍两个有关黎曼几何的结论:

(i) 在任何黎曼流形中,正交变换群的不动点子集总是一个全测地子流形.

(ii) 紧致连通黎曼空间 M 的任何两点都存在连结这两点的极短测地线.

令 $F(T,G)$ 是 $\widetilde{A}d|_T$ 在 G 上作用的不动点子集,则不难看出,T 是 $F(T,G)$ 的一个连通分支(其实 $T=F(T,G)$),但是这一点的证明要用到本定理,T 是 G 的一个全测地子流形.

设 $G(y)$ 是 G 中的一个任给的共轭类. 因为 $G(t_0)$ 和 $G(y)$ 是 G 中的两个紧致子流形,所以存在一条连结于两者之间的极短测地线. 它显然与 $G(t_0)$ 和 $G(y)$ 都是正交的(利用极短性即可证明). 设这样一条测地线段 γ 的端点分别是 $x_1\in G(t_0)$ 和 $y_1\in G(y)$,设 $x_1=gt_0g^{-1}$. 我们可以把这些测地线段 γ 用共轭 $\widetilde{A}d(g^{-1})$ 这个正交变换加以搬动,即得 $\widetilde{\gamma}=\widetilde{A}d(g^{-1})\gamma$(图 7.14). 它是一条过 t_0 点,垂直于 $G(t_0)$ 的测地线段,而且以 $y_0=g^{-1}y_1g\in G(y)$ 为其另一端点. 再者,因为 $\widetilde{\gamma}$ 和 T 相切(这是由于 $\widetilde{\gamma}\perp G(t_0)$ 且 $T\perp G(t_0)$),而 T 又是个全测地子流形,所以 $\widetilde{\gamma}\subset T$,这就证明了 T 与 $G(y)$ 至少交于一点,例如 y_0,但是 $G(y)$ 是任意一个共轭类,这也就证明了 T 和 G 中的任何共轭类都相交.

5) 设 T_1 是 G 中任给的另一极大子环群. 我们可以在 T_1 中取一个元素 t_1,使得它所生成的子群 $\langle t_1\rangle$ 在 T_1 中到处稠密,亦即 $\overline{\langle t_1\rangle}=T_1$. 由 4) 可知,存在 $g\in G$,使得 $gt_1g^{-1}\in T$,因此 $gT_1g^{-1}=g\overline{\langle t_1\rangle}g^{-1}=\overline{\langle gt_1g^{-1}\rangle}\subset T$.

由 T_1 和 T 的极大性可知 $gT_1g^{-1}=T$.

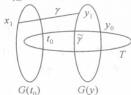


图 7.14

推论 7.6.4 一个紧致连通 Lie 群 G 的所有极大子环群的维数相同.

因此,我们可以定义 G 的秩为它的极大子环群的秩,也就是它的维数,记为 $\mathrm{rank}G(=\dim T)$.

推论 7.6.5 G 的一个子环群 T 是极大子环群的充要条件是它和 G 中的任何共轭类都相交.

定理 7.6.6 设 φ,ψ 是 G 任给的两个线性表示,T 是 G 的任一极大子环群. 令 $\psi|_T: TG \to GL(W)$,而 $\varphi|_T: TG \to GL(V)$,则 $\varphi \cong \psi$ 〗$\Leftrightarrow \varphi|_T \cong \psi|_T$.

证明 显然有 $\chi_\varphi|_T = \chi_{\varphi|T}, \chi_\psi|_T = \chi_{\psi|T}$. 又 χ_φ 和 χ_ψ 都是在 G 的任一共轭类上取等值的函数,而 T 又和 G 中任何的共轭类都相交,所以 $\chi_\varphi = \chi_\psi \Leftrightarrow \chi_\varphi|_T = \chi_\psi|_T$.

定理 7.6.7 设 S 是 G 的一个任给的子环群,$Z(S)$ 为 S 的中心化子,即 $Z(S) = \{g \in G; gsg^{-1} = s$,对所有 $s \in S\}$,则有 $Z(S) = \bigcup \{T', T' \supset S\}$,其中求并时 T' 取遍 G 的一切包含 S 的极大子环群. 由此可知 $Z(S)$ 是连通的. 特别地,一个极大子环群 T 的中心化子就是其本身.

证明 设 x 是 $Z(S)$ 中的任意一个元素,$< x,S >$ 表示由 x 和 S 生成的子群,$\overline{< x,S >}$ 是它的闭包. 则 $\overline{< x,S >}$ 显然是 G 中的一个可换闭子群. 它自然应该是 $< g_0 > \times S'$ 这种形式的群,其中 $S' \supset S$ 是一个子环群,而 g_0 是一个有限阶的元素,即 $g_0^m = e$(m 是某个正整数). 先取 $x_0 \in S'$,使得 $S' = \overline{< x_0 >}$,再取 $a \in S'$,使得 $a_m = x_0$. 令 $y = g_0 \circ a$,则有

$$y^m = g_0^m \circ a^m = e \circ x_0 = x_0, \text{所以} \overline{< y >} \supset \overline{< x_0 >} = S'.$$

这说明 $a \in \overline{< y >}$,从而 $g_0 = ya^{-1}$ 也属于 $\overline{< y >}$,即 $\overline{< y >} = < g_0 > xS' = \overline{< x,S >}$. 因为存在 g_1 使得 $g_1 y g_1^{-1} \in T$,亦即 $y \in g_1^{-1} T g_1$,所以 x 属于极大子环群 $g_1^{-1} T g_1$. 但是 x 是 $Z(S)$ 中的一个任意元素,所以 $Z(S) \subset \bigcup \{T'\}$,其中 T' 取遍 G 的所有包含 S' 的极大子环群. 再者,任何包含 S 的极大子环群 T' 自然应包含在 $Z(S)$ 中,于是推论得证.

推论的一个特殊情况就是 $Z(T) = T$,其中 T 是极大子环群. 换句话说 $F(T,G) = T$.

定义 7.6.3 令 $N(T,G) = \{g \in G; gTg^{-1} = T\}$,称之为 T 在 G 中的正规化子. 令 $W(G) = N(T,G)/T$,称之为 G 的 Weyl 群. 它是个作用在 $T = F(T,G)$ 上的变换群.

$W(G)$ 也可视为 T 的 Lie 代数 η 上的变换群. 事实上,对于 $g \in N(T,G)$,总有 $gTg^{-1} = T$,即 $\widetilde{A}d(G)T = T$,所以 $Ad(g)\eta \subset \eta$,且如图 7.15 所示图解可交换.

由此不难看出,

$$N(T,G) = \{g \in G; Ad(g)\eta \subset \eta\}, T = F(T,G) = \{g \in G; Ad(g)|_\eta = \mathrm{id}\}.$$

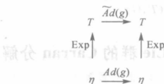


图 7.15

换句话说,$N(T,G)$ 也是 η(在 G 中)的正规化子,而 T 则是 η(在 G 中)的中心化子,所以 $W(G)$ 也是 η 上的变换群.

我们以符号 $G/\widetilde{A}d$, g/Ad 分别表示伴随变换群和伴随表示的轨道空间.以 $G/\widetilde{A}d$ 为例,$G/\widetilde{A}d$ 中的每个点都是由 G 中的一个共轭类所组成,即

$$\pi: G \to G/\widetilde{A}d$$

把每个轨道映射到一点,并取商拓扑.

再有,我们以 T/W 和 η/W 分别表示 T 和 η 在 $W(G)$ 作用下的轨道空间,则不难看出有如图 7.16 所示可换图解.

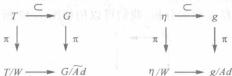


图 7.16

定理 7.6.8　在上述图解中,映射 $T/W \to G/\widetilde{A}d$ 和 $\eta/W \to g/Ad$ 都是一一在上的映射.

证明　因为 $\eta/W \to g/Ad$ 就起 $T/W \to G/\widetilde{A}d$ 的线性化和局部化,所以我们只需证明 $T/W \to G/\widetilde{A}d$ 是一一在上的映射.

首先,T 和 G 中任何共轭类都相交,这表明 $T/W \to G/\widetilde{A}d$ 是一个满射.下面,我们要证 明它也是一一对应.这也就是要证明下述事实:对于任给元素 $t_0 \in T$, $G(t_0) \cap T = W(t_0)$,这里 $W(t_0)$ 表示 t_0 在 $W(G_0)$ 作用之下的轨道.显然有

$$G(t_0) \cap T = G(t_0) \cap F(T,G) = F(T,G(t_0)).$$

又因为 $G(t_0) \cong G/G_{t_0}$, $G_{t_0} \supset T$,而且显然有

$$xG_{t_0} \in F(T,G/G_{t_0}) \Leftrightarrow xG_{t_0}x^{-1} \supset T \Leftrightarrow G_{t_0} \supset x^{-1}Tx,$$

所以我们只要证明,对于任给的 $xG_{t_0} \in F(T,G/G_{t_0})$,一定有一个元素 $n \in N(T,G)$,使得 $xG_{t_0} = nG_{t_0}$ 即可.由于 T 和 $x^{-1}Tx$ 都是 $G_{t_0}^0$ 的极大子环群,所以存在 $g \in G_{t_0}^0$,使得 $gTg^{-1} = x^{-1}Tx$,亦即 $(xg)^{-1}T(xg) = T$, $xg \in N(T,G)$,这就证明了

$$xG_{t_0} = (xg)G_{t_0},\ xg \in N(T,G).$$

§7.7　Lie 群的 Carran 分解

前面所证明的极大子环群定理是关于伴随变换的轨几何的基本定理，也是整个紧致 Lie 群论的枢纽. 本节将把这个定理和第一章的结果相结合，为系统地研讨紧致 Lie 群的结构论和表示论做好准备工作.

定义 7.7.1(权系)　设 $\varphi: G \to GL(V)$ 是一个给定的复表示. 已知 $\varphi|_T: T \subset G \to GL(V)$ 是 φ 的一个完全不变量. 但是 $\varphi|_T$ 又可以唯一地分解为一维复不可约表示的和，即

$$\varphi|_T = \varphi_1 \oplus \cdots \oplus \varphi_n, \qquad \dim \varphi_i = 1 (i = 1, \cdots, n).$$

上述 φ_i 都是一个由 T 到 $U(1) = S^1$ 的同态，而它的线性化 $\mathrm{d}\varphi_i$ 则是一个由 T 的 Lie 代数 η 到 $U(1)$ 的 Lie 代数 $\boldsymbol{R}^1$ 的 Lie 代数同态. 但是 η 和 $\boldsymbol{R}^1$ 都是可换的，亦即其上括积恒为零，所以 $\mathrm{d}\varphi_i$ 其实就是向量空间 η 到 $\boldsymbol{R}^1$ 的同态，即 η 上的线性函数，或者说，$\mathrm{d}\varphi_i \in \eta^*$（$\eta$ 的对偶空间 η）. 总结上面的分析，我们可以用如图 7.17 所示图解表达之.

$$\begin{array}{ccccc}
Z^r & \longrightarrow & Z^1 & & \\
\downarrow & & \downarrow & & \\
R^r \cong \eta & \xrightarrow{\mathrm{d}\varphi_i} & R^1 & \ni & 1 \\
\mathrm{Exp}\downarrow & & \downarrow\mathrm{Exp} & & 1 \\
T & \xrightarrow{\sigma_i} & U(1) = S^1 & \ni & e^{2\pi i t}
\end{array}$$

图 7.17

其中 $r = \mathrm{rank}(T) = \mathrm{rank}(G)$，亦即 $\varphi_i(\mathrm{Exp}H) = \exp\{2\pi i\mathrm{d}\varphi_i(H)\}$.

上面这种在 $\eta \cong \boldsymbol{R}^T$ 中的格点集 $\boldsymbol{Z}^T$ 上取整数值的线性函数 $\mathrm{d}\varphi_i$ 叫做整线性函数. 请注意，在上式的分解中，当然可能会有相互等价的，即存在不等的 i 和 j，使得 $\varphi_i = \varphi_j$，这种情形下也就有 $\mathrm{d}\varphi_i = \mathrm{d}\varphi_j$.

习惯上，我们可以把相同的 $\mathrm{d}\varphi_i$ 合并起来，标记以它们的重数. 这样，$\psi|_T$ 的分解就唯一地给出 η^* 中一个带有重数的子集，我们将以符号 $\Omega(\varphi)$ 表示之，叫做复表示 φ 的权系，它是 φ 的一组完全不变量. 且若 φ 是一个实表示，我们定义 $\Omega(\varphi) = \Omega(\varphi \otimes \boldsymbol{C})$，即以其复化后的权系为其权系：

$$(\varphi \otimes C: G \xrightarrow{\varphi} GL(V) \subset GL(V \otimes C),$$

或者说

$$G \xrightarrow{\varphi} GL(n,R) \subset GL(n,C)).$$

定义 7.7.2(根系)　设 G 是一个紧致连通 Lie 群,T 是 G 的一个选定的极大子环群. G 的伴随表示 Ad_G 的非零权,即 $Ad_G \otimes \boldsymbol{C}$ 的非零权,叫做 G 的根,而 Ad_G 的非零权的全体组成的集合,叫做 G 的根系,我们将以符号 $\triangle(G)$ 表示之.

$Ad_G \otimes \boldsymbol{C}$ 的零权的重数就是 $\mathrm{rank}(G)$. 而在下面我们将要证明它的所有非零权的重数都是 1. 因此,我们得知,$\triangle(G)$ 是 η^* 中一个不带重数的子集(每个根重数都是 1). 但是这要在证明了上述事实之后才可以这样说.

定义 7.7.3(Cartan 分解)　根系的定义乃是基于$(Ad_G|_T) \otimes \boldsymbol{C}$ 的分解,它是一个作用于 $g \otimes \boldsymbol{C}$ 上的 T- 变换群. 在上述 T 的作用之下,$g \otimes \boldsymbol{C}$ 可分解为下列不变子空间的直和,即

$$g \otimes \boldsymbol{C} = \eta \otimes \boldsymbol{C} + \sum_{a \in \Delta(G)} V_a, \quad \dim_{\boldsymbol{C}} V_a = a \text{ 的重数},$$

此分解式称为 g 的复 Cartan 分解,其中 T 在 $\eta \otimes \boldsymbol{C}$ 上的作用是平凡的,而 $\mathrm{Exp}H \in T$ 在 V_a 上的作用就是将其中每个向量乘以 $e^{2\pi i a(H)}$,亦即

$$Ad(\mathrm{Exp}H)X_a = e^{2\pi i a(H)} X_a, \qquad H \in \eta, X_a \in V_a.$$

其实,它是 $g \otimes \boldsymbol{C}$ 的一个分解式.

因为任何 T 的非平凡实不可约表示都是二维的,所以我们也可以直接把 g 本身加以分解,即有

$$g = \eta \oplus \sum_{\pm a \in \Delta(G)} m_a R^2_{(\pm a)},$$

此分解式称为 g 的实 Cartan 分解,其中 m_a 是根 a 在 $\triangle(G)$ 中的重数(以后将证明 $m_a = 1$),$m_a R^2_{(\pm a)}$ 是 m_a 个 $R^2_{(\pm a)}$ 的直和,而 T 在 $R^2_{(\pm a)}$ 上的作用如下:对于任给的 $H \in \eta$,$\mathrm{Exp}H \in T$ 在 $R^2_{(\pm a)}$ 上的作用是一个 $2\pi a(H)$ 角的旋转,亦即对于 $R^2_{(\pm a)}$ 中的一组正交基 X_a, Y_a 来说,$\mathrm{Exp}H$ 相应的矩阵为

$$\begin{pmatrix} \cos 2\pi a(H) & -\sin 2\pi a(H) \\ \sin 2\pi a(H) & \cos 2\pi a(H) \end{pmatrix}.$$

例 7.7.1　$G = S^3$. 前面已对于它的结构和复不可约表示做过详细的讨论. 现在把在那里所得的结果再用权系、根系的概念加以重述如下:

1) $S^1 = \{e^{2\pi i\theta}; 0 \leqslant \theta \leqslant 1\}$ 就是 S^3 的一个极大子环群.

2) 将 S^3 到 $SU(2)$ 的同构映射 φ_1 限制到 S^1 上,即得

$$\varphi_1|_{S^1}: S^1 \to SU(2); e^{2\pi i\theta} \longmapsto \begin{pmatrix} e^{2\pi i\theta} & 0 \\ 0 & e^{-2\pi i\theta} \end{pmatrix}.$$

如果仍用 θ 及 $-\theta$ 表示 $\boldsymbol{R}^1$ 上的线性函数 $\theta(t) = t$ 以及 $(-\theta)(t) = -t (t \in \boldsymbol{R})$,则

由权系的定义即有 $\Omega(\varphi_1)=\{\theta,-\theta,$重数均为$1\}$.

3)S^3 的伴随表示 $Ad_{S^3}:S^3\to SO(3)$ 是一个三维实表示，它的复化 $Ad_{S^3}\otimes C$ 则是一个三维复不可约表示，而 S^3 的三维复不可约表示在等价意义下是唯一的，即 φ_2，因此 $Ad_{S^3}\otimes C\cong\varphi_2$. 由 φ_2 的定义不难得出

$$\varphi_2|_{S^1}:S^1\to U(3);e^{2\pi i\theta}\longmapsto\begin{pmatrix}e^{4\pi i\theta}&0&0\\0&0&0\\0&0&e^{-4\pi i\theta}\end{pmatrix}.$$

所以 $\Omega(\varphi_2)=\{2\theta,0,-2\theta\}$，因此 $\triangle(S^3)=\{2\theta,-2\theta\}$. 换句话说，$S^3$ 只有一对根，一正一负，互为相反，重数为 1.

4) 同理可得 S^3 的任一复不可约表示 φ_k(k 为正整数) 的权系是

$$\Omega(\varphi_k)=\{k\theta,(k-2)\theta,\cdots,-(k-2)\theta,-k\theta\},$$

权的重数皆为 1，它们构成一个由 $k\theta$ 到 $-k\theta$ 的“等差向量列”，其公差为 2θ，这恰是 S^3 的唯一正根.

例 7.7.2　$G=SO(3)$. S^3 的伴随表示 $Ad:S^3\to SO(3)$ 是一个三维实不可约表示，它的核 $Ad^{-1}(e)=\{\pm 1\}$，因此 $S^3/\{\pm 1\}\cong SO(3)$.

这表明 Ad 是一个覆盖同态. 由此可知，$SO(3)$ 也是秩一的，而且有如图 7.18 所示图群.

$$\begin{array}{ccccc}
\{\theta\}=R^1 & \longrightarrow & R^1=\{\theta'\} & \cong & \left\{\begin{pmatrix}0&-\theta'&\\ \theta'&0&\\ &&0\end{pmatrix}\right\}\\
\downarrow\ \mathrm{Exp} & & \downarrow\ \mathrm{Exp} & & \downarrow\\
\{e^{2\pi i\theta}\}=S^1 & \longrightarrow & SO(2) & \cong & \left\{\begin{pmatrix}\cos 2\pi i\theta' & -\sin 2\pi i\theta' & \\ \sin 2\pi i\theta' & \cos 2\pi i\theta' & \\ && 1\end{pmatrix}\right\}\\
n\downarrow & & \downarrow n & & \\
S^3 & \xrightarrow{Ad} & SO(3)\cong S^3/\{\pm 1\} & &
\end{array}$$

图 7.18

在上述图解中，映射 $\boldsymbol{R}^1\to\boldsymbol{R}^1$ 将 $\theta\longmapsto\theta'=2\theta$，其中 θ 和 θ' 分别是 S_1 和 $SO(2)$ 的基准参数. 利用上述覆盖同态，我们可以把 $SO(3)$ 的任何一个表示 $\psi:SO(3)\to GL(V)$ 提升为一个 S^3 的表示，即

$$\varphi=\psi\circ Ad_{S^3}:S^3\xrightarrow{Ad}SO(3)\to GL(V).$$

它是一个满足 $\ker(\varphi)\supset\{\pm 1\}$ 的表示.

反之，S^3 的任何满足 $\ker(\varphi)\supset\{\pm 1\}$ 的表示 $\varphi:S^3\to GL(V)$ 也都可以压缩成一个 $SO(3)$ 的表示，使得 $\varphi=\psi\circ Ad_{S^3}$. 我们可以用如图 7.19 所示的图解表明上述关系.

除了 φ 是平凡表示的特殊情形外，均有 $\ker(\varphi)\subset S^1$，而且只有 $\ker(\varphi)=\{1\}$ 和

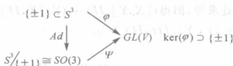


图 7.19

$\ker(\varphi) = \{\pm 1\}$ 这两种可能. 也就是说, $\ker(\varphi) = \ker(\varphi|_{S^1})$. 而 $\ker(\varphi) = \{\pm 1\}$ 的充分必要条件是权系 $\Omega(\varphi)$ 中所含的向量都是 θ 的偶数倍. 所以, 从权系的观点来看, 上述相应的线性表示 φ 和 ψ 之间的关系就是

$$\begin{cases} \Omega(\varphi) \text{ 中所含的向量都是 } 2\theta \text{ 的整数倍}, \\ \Omega(\psi) \text{ 就是把 } \Omega(\varphi) \text{ 中的 } 2\theta \text{ 改写成 } \theta' \text{ 者}. \end{cases}$$

在 S^3 的所有复不可约表示 $IR(S^3) = \{\varphi_k; k = 0,1,2,\cdots\}$ 之中, 当且仅当 k 是偶数 $2l$ 时, $\ker(\varphi_k) = \{\pm 1\}$. 所以

$$\begin{cases} IR(SO(3)) = \{\psi_l; l = 0,1,2,\cdots, \phi_{2l} = \psi_l \circ Ad\}, \\ \Omega(\psi_l) = \{l\theta', (l-1)\theta', \cdots, -l\theta'\}, \text{重数皆为 } 1. \end{cases}$$

例 7.7.3　S^3 和 $SO(3)$ 的 Lie 代数. 由于 $S^3 \to SO(3)$ 是覆盖同态, 所以两者的 Lie 代数是同构的, 我们将以 α_1 表示之. α_1 是一个三维秩一的不可换 Lie 代数, 它的实 Cartan 分解式为

$$\alpha_1 = R^1 \oplus R^2_{(\pm\theta)} (\text{或 } R^1 \oplus R^2_{(\pm 2\theta)}).$$

我们可以在 $\boldsymbol{R}^1$ 中选取基底 H, 使得

$$Ad(\mathrm{Exp}H) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \in SO(2),$$

并且令 X, Y 是 $R^2_{(\pm\theta')}$ 中的一组相应的正交基底, 则有

$$\begin{cases} \mathrm{Exp}(t\,adH) \cdot X = Ad(\mathrm{Exp}tH) \cdot X = (\cos t)X + (\sin t)Y, \\ \mathrm{Exp}(t\,adH) \cdot Y = Ad(\mathrm{Exp}tH) \cdot Y = (-\sin t)X + (\cos t)Y. \end{cases}$$

将上式左、右两边分别对 t 求导, 然后代以 $t = 0$, 即得

$$\begin{cases} [H, X] = adH \cdot X = Y, \\ [H, Y] = adH \cdot Y = -X. \end{cases}$$

因此, 再利用 Jacobi 恒等式, 我们便得到

$$[[X,Y],H] = -[[H,X],Y] - [[Y,H],X] = 0.$$

$[X,Y]$ 与 H 必定线性相关. 要不然, α_1 中就有一个二维的可换子代数, 这显然与 α_1 是秩一的事实相违背. 设 $[X,Y] = \lambda H$, 我们要说明 $\lambda > 0$. 令 $(,)$ 为 α_1 上任取的一个 Ad-不变内积, 则有

$$(Ad(\mathrm{Exp}tX)Y, Ad(\mathrm{Exp}tX)H) \equiv (Y, H) (\text{与 } t \text{ 无关}).$$

将此式对 t 在 $t=0$ 处求导，即得 $([X,Y],H)+(Y,[X,H])=0$，亦即 $(\lambda H,H)+(Y,-Y)=0$，从而 $\lambda=(Y,Y)/(H,H)>0$.

再令

$$X_1=\frac{1}{\sqrt{\lambda}}X, Y_1=\frac{1}{\sqrt{\lambda}}Y, \text{即有} \begin{cases}[H,X_1]=Y_1,\\ [H,Y_1]=-X_1,\\ [X_1,Y_1]=H.\end{cases}$$

这样一组基底 $\{H,X_1,Y_1\}$ 叫做 Lie 代数 α_1 的标准基底.

定理 7.7.1　设 G 为一个任给的紧致连通 Lie 群，若 $\text{rank}(G)=1$，则 G 必与 S^1，S^3 或 $SO(3)$ 中之一同构.

证明　因为所有的可换秩一紧致连通 Lie 群都和 S^1 同构，所以我们只需要讨论 G 是不可换的情形. 设 T^1 是 G 的一个极大子环群，由假设 $\text{rank}(G)=1$，所以 T^1 是一阶的，我们采用参数 $0\leqslant t\leqslant 2\pi$ 来表达 T^1 中的元素，亦即 $T^1\cong R^1/\{2\pi\mathbf{Z}\}$.

设 g 的实 Cartan 分解为

$$g=R^1\oplus R^2_{(n_1)}\oplus\cdots\oplus R^2_{(n_k)},$$

由参数的选取可知，$n_1,\cdots,n_k$ 均为正整数，而 $R^2_{(n_i)}(1\leqslant i\leqslant k)$ 就是 $Ad_G|_{T^1}$ 的不可约子空间，而且 T^1 在 $R^2_{(n_i)}$ 上的表示是：

$$h_i: T^1\to SO(2), h_i(t)=\begin{pmatrix}\cos n_it & -\sin n_it\\ \sin n_it & \cos n_it\end{pmatrix},$$

我们不妨假设上述正整数集 $\{n_i,1\leqslant i\leqslant k\}$ 满足 $n_1\leqslant\cdots\leqslant n_k$.

参照例 7.7.3 的讨论，我们可以分别取 R^1 和 $R^2_{(n_1)}$ 的基底 H 和 $\{X,Y\}$，使得

$$\begin{cases}Ad(\text{Exp}H)X=(\cos n_1t)X+(\sin n_1t)Y,\\ Ad(\text{Exp}tH)Y=(-\sin n_1t)X+(\cos n_1t)Y.\end{cases}$$

同样地，将上式对 t 在 $t=0$ 处微分，就得出

$$[H,X]=n_1Y \quad \text{和} \quad [H,Y]=-n_1X.$$

令

$$H'=\frac{1}{n_1}H, \text{则有}[H',X]=Y \text{和}[H',Y]=-X.$$

从这里，就可以改取

$$X'=\frac{1}{\sqrt{\lambda}}X, Y'=\frac{1}{\sqrt{\lambda}}Y(\text{其中}[X,Y]=\lambda H',\lambda>0),$$

即得括积关系

$$\begin{cases}[H',X']=Y',\\ [H',Y']=-X',\\ [X',Y']=H'.\end{cases}$$

将此式与前式相对比，就看出由 H', X', Y' 张成的子代数 g_1 是一个与 α_1 同构的 Lie 子代数！在 G 中含有一个与 S^3 或 $SO(3)$ 同构的 Lie 子群 G_1，它的 Lie 代数就是上述 g_1.

到此为止，本定理的证明也就归结到要去证明 G 必须等于 G_1. 换句话说，就是要从假设 G 真包含 G_1 得出矛盾. 兹证之如下：设 g 真包含 g_1. 将 Ad_G 在 g 上的作用限制到 G_1 上，则 g_1 显然是 G_1- 不变的，所以 g_1 的正交补空间

$$g_1^{\perp} = R^2_{(n_2)} \oplus \cdots \oplus R^2_{(n_k)}$$

当然也是 G_1 不变的. 现在分 $G_1 \cong S^3$ 和 $G \cong SO(3)$ 这两种情形来讨论.

1) 若 $G_1 \cong S^3$，则上述 G_1 在 $g_1^{\perp} \otimes C$ 上的作用就是 S^3 的一个复表示

$$\varphi: S^3 \to U(2k-2).$$

因为 $n_i \geqslant n_1 (i = 2, \cdots, k)$，所以权系 $\Omega(\varphi)$ 中的向量不是 $\geqslant 2\theta$，就是 $\leqslant -2$.

换句话说，$\Omega(\varphi)$ 中不含有任何向量 w，$-2\theta < w < 2\theta$. 但是，由例 7.7.1 的讨论可知，$\Omega(\varphi)$ 必须是由某些对称的、公差为 2θ 的等差向量列所合并而成的，所以当然不可能出现像上面这种跨度为 4θ 的间隙！因此这种情形不可能出现.

2) 若 $G \cong SO(3)$，则上述 G_1 在 $g_1^{\perp} \otimes C$ 的作用就是 $SO(3)$ 的复表示

$$\psi: SO(3) \to U(2k-2),$$

而它的权系不含有零权，这与例 7.7.2 的结果相矛盾（因为 $SO(3)$ 的任何复不可约表示的权系一定含有零权，参看例 7.7.2）.

总之，G 真包含 G_1 这种假设是绝对不可能的，所以只能是 $G = G_1$.

定理 7.7.2　设 $\triangle(G)$ 是紧致连通 Lie 群 G 的根系，则其中的任何一个根 α 的重数都是 1，而且 $k\alpha \in \triangle(G)$ 的充要条件是 $k = \pm 1$.

证明　由权的定义，$\alpha: R^k = \eta \to R^1$ 是 η 上的一个整线性函数. 令 T_α 是以 $\ker(\alpha)$ 为其 Lie 代数的子环群，且令

$$\begin{cases} G_\alpha = Z(T_\alpha, G) = \{g \in G; gt = tg, \forall\, t \in T_\alpha\}, \\ \widetilde{G}_\alpha = G_\alpha / T_\alpha. \end{cases}$$

令 g_α 和 $\widetilde{g}_\alpha$ 分别是 G_α 和 $\widetilde{G}_\alpha$ 的 Lie 代数. 不难验证

$$g_\alpha = \{X \in \eta; Ad(t)X = X, \forall\, t \in T_\alpha\} = \{X \in g; [H, X] = 0, \forall\, H \in \ker(\alpha)\}.$$

于是由 g 的实 Cartan 分解就不难看出 g_α 及 $\widetilde{g}_\alpha$ 的实 Cartan 分解应是：

$$g_\alpha = \eta \oplus \sum_{\beta = k\alpha} m_\beta R^2_{(\pm\beta)},$$

$$\overline{g}_\alpha = \eta / \mathrm{Ker}(\alpha) \oplus \sum_{\beta = k\alpha} m_\beta R^2_{(\pm\beta)} \cong R^1 \oplus \sum_{\beta = k\alpha} m_\beta R^2_{(\pm\beta)}.$$

在上式中，取一切与 α 线性相关的根（亦即 $\ker\beta = \ker\alpha$ 者），所以 $\widetilde{G}_\alpha$ 是一个秩一的

紧致连通 Lie 群，知 $\dim\widetilde{g}_\alpha = 3$，从而 $\beta = \pm\alpha$，且 $m_\alpha = m_{-\alpha} = 1$.

为了便于运用几何术语来描述根系的结构，我们将从现在开始，在 g 上取定一个 Ad_G-不变的内积，然后利用其局限于 η 上的内积结构把 η^* 与 η 对等起来，亦即 η^* 到 η 的同构映射

$$\iota:(\tau(\alpha), H) = \alpha(H)$$

对任何 $\alpha \in \eta^*$ 及 $H \in \eta$ 恒成立. 这样，就可以把原先是 η^* 中的子集 $\triangle(G)$ 和 η 中的子集 $\iota(\triangle(G))$ 对等起来. 而我们从现在开始，就把根系的定义更新为上述 η 中的子集. 所以，今后 $\triangle(G)$ 是 η 中一个不带重数的(因为每个根 α 的重数皆为1) 的非零向量子集. 当然，在改用根系的新定义之后，原先用以描述复 Cartan 分解的公式就得改写为

$$Ad(\mathrm{Exp}H)X_\alpha = e^{2\pi i(\alpha,H)}X_\alpha,\quad H \in \eta, X_\alpha \in V_\alpha.$$

而原先的 $\ker(\alpha)$ 就可以改写为 $(\alpha)^\perp$，即 α 的正交补空间.

为进一步讨论根系的性质，我们对 G_α 的表示 $Ad_G|_{G_\alpha}$ 作进一步的分析：

1) 对于 $\triangle(G)$ 中任给的一对根 $\{\pm\alpha\}$，G_α 是一个和 G 本身同秩的紧致连通 Lie 群，其根系和 Lie 代数分别是：

$$\begin{cases}\triangle(G_\alpha) = \{\pm\alpha\},\\ g_\alpha = \eta \oplus R^2_{(\pm\alpha)} = <\alpha>^\perp \oplus <\alpha> \oplus R^2_{(\pm\alpha)} = <\alpha>^\perp \oplus \widetilde{g}_\alpha,\end{cases}$$

其中 $\widetilde{g}_\alpha = <\alpha> \oplus R^2_{\pm\alpha}$ 是一个和 α_1 同构的三维 Lie 代数，所以存在一个由 $T_\alpha \times S^3$ 到 G_α 的覆盖同态 $p: T_\alpha \times S^3 \to G_\alpha$.

2) 当我们将 G 在 $g \otimes C$ 上的伴随表示限制到 T 上时，$g \otimes C$ 的 T-不可约直和分解就是它的复 Cartan 分解.

$$g \otimes C = \eta \oplus C \oplus \sum_{\alpha\in\triangle(G)} V_\alpha,\ \dim V_\alpha = 1.$$

上述 G_α 是一个介于 G 与 T 之间的子群. 所以在 $Ad_G|_{G_\alpha}$ 的作用下，$g \otimes C$ 的 G_α-不可约直和分解可以说是上述复 Cartan 分解的前身. 换句话说，$g \otimes C$ 中的任一 G_α-不可约子空间都是由上分解式中的某一适当部分合并而成. 再者，如同例 7.7.2 的讨论一样，我们也可以把 G_α 的一个复不可约表示 ψ 用覆盖同态 ρ 把它提升成一个 $T_\alpha \times S^3$ 的复不可约表示 $\varphi = \psi \cdot \rho$. 这样就有 $T_\alpha \times S^3$ 的复不可约表示都有下列形式：$\rho \hat{\otimes} \varphi_i$，其中 ρ 是 T_α 的一个复一维表示，它的权是 $<\alpha>^\perp$ 中一个向量，而 φ_i 是 S^3 的 $(i+1)$ 维复不可约表示，它的权系是一个公差为 α(S^3 的唯一正根) 的等差向量列，它们都在子空间 $<\alpha>$ 中，且对于 $<\alpha>^\perp$ 成反射对称. 另一方面，由权与特征值的关系以及作张量积时特征值相乘这一基本事实不难看出，$\rho \hat{\otimes} \varphi_i$ 的权系与 φ_i 的权系以及 ρ 的权之间的关系可以用图 7.20 表示. 因此，

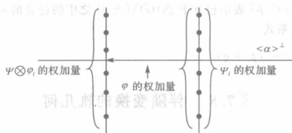


图 7.20

$\rho\otimes\varphi_i$ 亦即 $T_\alpha\times S^3$ 的复不可约表示的权系也是一个公差为 α，关于 $<\alpha>^{\perp}$ 成反射对称的 α- 等差向量列. 以后简称为 α- 等差向量列.

3) 因为 g_α 当然是 G_α- 不变的，所以我们可以先把 $g\otimes C$ 分解成下述三个不变子空间的直和，即

$$g\otimes C=<\alpha>^{\perp}\otimes C\oplus\widetilde{g}_\alpha\otimes C\oplus\sum_{\substack{\beta\neq\pm\alpha\\ \beta\in\triangle(G)}}V_\beta.$$

再者，若 U 是包含 V_β 的那个 G_α- 不可约子空间，则 (G_α,U) 这个复不可约表示的权系必构成一个 α- 等差向量列 $\{\beta+j\alpha;q\leqslant j\leqslant p\}$，而且 $\beta+p\alpha$ 与 $\beta+q\alpha$ 关于 $<\alpha>^{\perp}$ 对称. 由于关于 $<\alpha>^{\perp}$ 的对称 r_α 可表为

$$r_\alpha(\xi)=\xi-\frac{2(\xi,\alpha)}{(\alpha,\alpha)}\alpha,$$

所以 $$\beta+q\alpha=r_\alpha(\beta+p\alpha)=(\beta+p\alpha)-\frac{2(\beta+p\alpha,\alpha)}{(\alpha,\alpha)}\alpha,$$

即 $$(p+q)\alpha=-\frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha,\frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha=-(p+q).$$

请参看图 7.21 所示.

又因为 V_i 的维数都是 1，不难看出，$\triangle(G)$ 中除了上述 α- 等差向量列之外，就不可能再含有其他也能写成 $\beta+j\alpha$ 形式的根了！

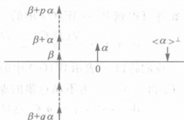


图 7.21

总结上述三点分析，即有下述定理：

定理 7.7.3　在 $Ad_G|_{G_\alpha}$ 的作用之下，$g\otimes C$ 的完全分解如下：

$$g\otimes C=<\alpha>^{\perp}\otimes C\oplus\widetilde{g}_\alpha\otimes C\oplus\sum_\beta\Big(\sum_{j=q}^{p}V_{\beta+j\alpha}\Big),$$

其中$\{\beta + j\alpha; q \leqslant j \leqslant p\}$表示包含于$\triangle(G)\setminus\{\pm\alpha\}$之中的过$\beta$的$\alpha$-向量列. 再者,我们还有下述重要关系式

$$\frac{2(\alpha,\beta)}{(\alpha,\alpha)} = -(p+q).$$

§7.8 伴随变换的轨几何

在本章开始,我们就指出了伴随变换的轨几何在群论研究中的重要性. 例如,在$G = S^3$这个实例中,我们可以把它想成是$\boldsymbol{Q} \cong \boldsymbol{R}^4$中的单位球面,则其伴随变换就可以看作是以实数轴为转轴的$SO(3)$旋转变换. 所以S^3的伴随变换的轨几何是简明易算的.

本节将在前面结果的基础上,把前面对于S^3上的共轭类几何的这种了解,推广到一般紧致连通 Lie 群的范围. 有了这种了解,就可以直截了当地得出紧致连通 Lie 群表示论的基本定理.

1) 已知下述基本事实:

$$G/\widetilde{A}d \cong T/W,\ g/Ad \cong \eta/W,$$

且$T \subset G$和$\eta \subset g$都分别是G和g的全测地子流形,而且它们又都分别与G和g中的任一轨道正交. 这也说明了,G或g上的轨几何的法向部分是可以转化为(W,T)或(W,η)的轨几何来加以理解与计算的.

2) 由于特征函数的积分计算在群表示论中所占的重要地位,讨论G的共轭类几何的切向部分的重点显然应该是:如何有效地计算各共轭类的体积,并且把它们组织成一个体积函数在S^3的情形,这个体积函数就是$c\sin t$.

3) 对于任给的$\{\pm\alpha\} \subset \triangle(G)$,显然有

$$T \subset N(T,G_\alpha) \subset N(T,G),$$

由此即可得到$W = W(G)$中的一个二阶子群

$$W(G) = \frac{N(T,G)}{T} \supset \frac{N(T,G_\alpha)}{T} = W(G_\alpha) \cong \boldsymbol{Z}_2\ .$$

我们将以r_α表示$W(G_\alpha)$中的那个二阶元素,不难看出它在T和η上的作用是分别以T_α和$<\alpha>^\perp$为不动点集的那个反射对称. 令

$$W' = < r_\alpha;\ \pm\alpha \in \triangle(G) >$$

是W中由所有r_α这种反射对称所生成的子群. 我们将证明$W' = W$.

4) 由于$W' = W$,所以(W,T)是一个反射变换群. 对每个反射对称r_α,它的不动点点集$F(r)$是余一维的,而且每个$F(r)$把全空间分成两个不相交的部分. 而开集$T\setminus \bigcup_{r\in\triangle} F(r)$是一块块连通开集的并集,每一个连通区域$C$,就叫做一个 Weyl 房. 可以证

明 W 在 Weyl 房组成的集合上的作用是单可递的. 因此，我们只要在 T 中任取一个 Weyl 房 C_0，则 $\overline{C}_0$ 构成 (W,T) 的一个基本域. 所以

$$G/\widetilde{A}d \cong T/W \cong \overline{C}_0,$$

亦即 $\overline{C}_0$ 和 G 中的任一共轭类都相交于且仅交于一点 1，而且对于任一个内点 $t_0 \in C_0$，均有 $W_{t_0} = \{e\}, G_{t_0} = T$.

基于上述分析，我们有

定理 7.8.1 $W(G) = N(T,G)/T$ 在 T 和 η 上的作用都是反射变换群，亦即它就是由反射对称 $< r_\alpha;\ \pm\alpha \in \triangle(G) >$ 所生成的群.

证明 在上面的分析 3) 中已经指出 W 包含那个由反射对称

$$< r_\alpha;\ \pm\alpha \in \triangle(G) >$$

所生成的子群 W'，所以我们只要证明 $W' \supset W$ 即可. 另一方面，因为 (W, η) 是 (W,T) 的局部化和线性化，所以只讨论前面的情形也足够了.

假设 $W \underset{\neq}{\supset} W'$. 因为 W' 在 Weyl 房的集合上是单可递的，所以一定有 W 中的元素 $\sigma \neq e$ 及一个 Weyl 房 C_0，使得 $\sigma(C_0) = C_0$. σ 是正交变换，所以 σ 在 C_0 上的作用一定有不动点 x_0. 由于 x_0 是 C_0 中的点，自然是一个内点，而且 σ 不是单位元素，且 $G_{x_0}^0 = T$ 但 G_{x_0} 本身非连通. 另一方面，G_{x_0} 是单参数子群 $\{\mathrm{Exp}tX_0; t \in \boldsymbol{R}\}$ 的中心化子，亦即是它的闭包 $S = \{\mathrm{Exp}tX_0\}$ 这个子环群的中心化子 $\boldsymbol{Z}(S)$，但是 $\boldsymbol{Z}(S)$ 是连通的，即 G_{x_0} 连通，这与上述 G_{x_0} 非连通性矛盾，所以只能 $\sigma = e$ 且 $W = W'$.

为了建立 Weyl 的积分公式，我们先给一些定义，这对以后的讨论也很有用处. 设 η 是 T 的 Lie 代数. 在 η 上我们选取一个向量之间的大小次序（例如按 η 上某个坐标系建立起来的字典排列法，即若 $\alpha, \beta \in \eta$，α, β 对某个取定的坐标系来说，坐标分别是 $(x_1, \cdots, x_k)$ 和 $(y_1, \cdots, y_k)$，则 $\alpha > \beta$ 当且仅当对某个 $i(1 \leqslant i \leqslant k)$，总有 $x_j = y_j(j < i$ 且 $x_i > y_i)$. 对这种取定的次序，把 $\triangle(G)$ 中的所有根分成两类，即 $\alpha > 0$ 及 $\alpha < 0$，分别称为正根和负根. 所有正根的集合记为 $\triangle^+$（叫正根系），所有负根集合记为 $\triangle^-$（叫负根系），于是 $\triangle(G) = \triangle^+ \cup \triangle^-$. 不仅如此，令

$$C_0 = \{H \in \eta; (\alpha, H) > 0, \forall\ \alpha \in \triangle^+\}.$$

不难验证 C_0 是一个 Weyl 房，称之为相应于上述次序的基本 Weyl 房. 在 $\triangle^+$ 中，使得 $C_0 = \{H \in \eta; (\alpha_i, H) > 0, \alpha_i \in \pi\}$ 成立的极小子集 π，叫做相应于这个次序的素根系. 不难证明：素根系构成 η 的一组基底，每个正根 α 均可表为 $\alpha_1, \cdots, \alpha_k$ 的非负整线性组合.

定理 7.8.2（Weyl 积分公式） 设在紧致连通 Lie 群 G 中业已取定了总体积为 1 的左、右不变的黎曼结构，f 为其上任何一个中心函数（亦即在任何共轭类上皆取等值的函数，或者说是 $\widetilde{A}d$ 不变函数），则有下列 Weyl 积分公式：

$$\int_G f(g)\mathrm{d}g = \frac{1}{|W|}\int_T f(t)\,|Q(t)|^2\mathrm{d}t,$$

其中 $|W|$ 表示 W 中元素个数，当 $t = \mathrm{Exp}H(H \in \eta)$ 时，$Q(t)$ 可以用下式表达：

$$Q(\mathrm{Exp}H) = \sum_{\sigma\in W}\mathrm{sign}(\sigma)\mathrm{e}^{2\pi i(\sigma(\delta),H)},$$

其中 δ 是所有对于 C_0 而言的正根之和的一半，亦即 $\delta = \dfrac{1}{2}\sum_{\alpha\in\triangle^+(G)}\alpha.$

证明 1) 从上面关于 G 上 $\widetilde{A}d$ 的轨几何的分析，我们知道 T 是一个全测地子流形，而且和每个共轭类都正交. 再者，$\overline{C}_0 \cong T/W \cong G/\widetilde{A}d$，是一个优良的基本域，其上任给两点 t_1 和 t_2，它们在 $\overline{C}_0$ 中的距离也就是共轭类 $G(t_1)$ 和 $G(t_2)$ 在 G 中的最短距离，简称之为轨距离.

2) 对于任给内点 $t \in \mathrm{C}_0$，其轨道型皆为 G/T. 但是对于任给的边界点 $t \in \partial\overline{C}_0 = \overline{C}_0\backslash C_0$，则其轨道的维数恒小于 $\dim G/T$，所以所有非 G/T 型轨道的并集，即

$$G(\partial\overline{C}_0) = \bigcup_{x\in\partial\overline{C}_0} G(x)$$

的测度为零. 换句话说，在 G 上求积分时，上述子集 $G(\partial\overline{C}_0)$ 可以略去不计，只要在 $G(C_0)$ 上计算之即可.

3) 令 t 为 C_0 上的一个动点，$m = \dim G/T = \dim G - \dim T$，则 $G(t)$ 为 $G(t)$ 型的轨道，而它的 m 维体积就是一个以 C_0 为其定义域的函数，称之为（主型）轨体积函数，记为 $v(t)$. 因为每个轨道 $G(t)$ 都是同样的 G/T 型齐性黎曼空间，所以它们的体积之比就等于其体积元素之比. 我们可以取定一个基准的 G/T 型齐性黎曼空间，对于每一个 G/T 型轨道 $G(t)$，把陪集 $g\cdot T$ 映射到 $g(t)$ 就是一个同型的齐性黎曼空间之间的 G- 等变映射 E_t①

$$E_t : G/T \to G(t),$$

$$G\cdot T \mapsto g(t) = gtg^{-1},$$

则上述两者的"体积元素"之比也就是上述映射 E_t 的 Jacobi 行列式，亦即 E_t 在基点的切空间所诱导的线性映射的行列式. 这就是说，所要去求的体积函数 $v(t)$ 可以由下式来计算之：

$$v(t) = c\cdot\det(\mathrm{d}E_t|_0),$$

其中 c 是一个待定的比例常数，而 $\mathrm{d}E_t|_0$ 是基点的切空间上的线性映射

$$\mathrm{d}E_t|_0 : \bigoplus\sum_{\alpha\in\triangle^+} R^2_{(\pm\alpha)} \to \mathscr{T}_0(G(t)).$$

4) 因为 E_t 是 G- 等变的，所以 $\mathrm{d}E_t|_0$ 是 T- 等变的（因为基点是在 T 的作用之下的不动点）. 因此 $\mathrm{d}E_t|_0$ 可以分解为下述二维 T- 不变子空间的线性映射的直和：

$$\mathrm{d}E_t|_{0,\alpha} : R^2_{(\pm\alpha)} \to \mathscr{T}_0(G(t)).$$

所以就可以用下式来计算 $\det(\mathrm{d}E_t|_0)$：

$$\det(\mathrm{d}E_t|_0)=\prod_{\alpha\in\triangle^+}\det(\mathrm{d}E_t|_{0,\alpha}).$$

另一方面，$\det(\mathrm{d}E_t|_{0,\alpha})$ 又是和 $G_\alpha/T_\alpha=\widetilde{G}_\alpha\subseteqq S^3$ 中的 S^3-型（主）轨体积函数成比例者，即可以运用下面的图解：

$$\begin{array}{ccc} G_\alpha/T & \xrightarrow{E_{t,\alpha}} & G_\alpha(t)\subset G_\alpha/t_\alpha=\widetilde{G}_\alpha \\ \cap & & \cap \\ G/T & \xrightarrow{E_t} & G(t)\subset G \end{array}$$

$\det(\mathrm{d}E_t|_{0,\alpha})$ 的计算又归于 $\widetilde{G}_\alpha$ 中 S^2-型的体积函数（由于 $\widetilde{G}_\alpha$ 或与 S^3 同构，或与 $SO(3)$ 同构，所以 $\widetilde{G}_\alpha$ 与 S^3 有相同的体积元素，从而在上述问题中可以视 $\widetilde{G}_\alpha$ 是 S^3），这种体积函数在前面已讨论过，于是我们有

$$\det(\mathrm{d}E_t|_{0,\alpha})=c'\cdot\sin^2\pi(\alpha,H),$$

其中 H 满足 $t=\mathrm{Exp}H$（注意，S^3 的正根是 2θ），综合上面各式，得出

$$v(\mathrm{Exp}H)=c''\circ\prod_{\alpha\in\triangle^+}\sin^2\pi(\alpha,H)=c\circ|\widetilde{Q}(\mathrm{Exp}H)|^2,$$

其中

$$\widetilde{Q}(\mathrm{Exp}H)=\prod_{\alpha\in\triangle^+}(\mathrm{e}^{\pi i(\alpha,H)}-\mathrm{e}^{-\pi i(\alpha,H)}).$$

5）最后我们要证明上式中的 $\widetilde{Q}(\mathrm{Exp}H)=Q(\mathrm{Exp}H)$.

证明 设 $\{\alpha_1,\alpha_2,\cdots,\alpha_k\}$ 是对于 Weyl 房 C_0 来说的素根系，则由反射对称的定义可知，$r_{\alpha_i}(\alpha_i)=-\alpha_i$，这相当于被 $\langle\alpha_i\rangle^\perp$ 所划分出的两个半空间正负侧选取的改变，它自然对于其他正根 α 所对应的，由 $\langle\alpha\rangle^\perp$ 所划分的两个半空间正负侧选取无影响，所以在 r_{α_i} 下 $\triangle^+\setminus(\alpha_i)$ 仍变为 $\triangle^+\{\alpha_i\}$，于是有

$$r_{\alpha_i}(\triangle^+)=(\triangle^+\setminus\{\alpha_i\})\cup\{-\alpha_i\}(1\leqslant i\leqslant k).$$

上式也可由 r_{α_i} 的表达式出发通过直接计算反正根是素根系非负整线性组合这个事实给出一个代数的证明.

设 $\delta=\frac{1}{2}\sum_{\zeta\in\triangle^+}\alpha_\zeta$，由上式可知，$r_{\alpha_i}(\delta)=\delta-\alpha_\zeta$，且

$$r_{\alpha_\zeta}(\delta)=\delta-\frac{2\langle\delta,\alpha_i\rangle}{\langle\alpha_i,\alpha_i\rangle}\alpha_i,1\leqslant i\leqslant k,$$

因此

$$\frac{2\langle\delta,\alpha_i\rangle}{\langle\alpha_i,\alpha_i\rangle}=1.$$

又由 $\widetilde{Q}(\mathrm{Exp}H)$ 的表达式及前式马上推知，

$$\widetilde{Q}(\mathrm{Exp}r_{\alpha_i}(H)) = (-1)\cdot\widetilde{Q}(\mathrm{Exp}H).$$

因此，对 W 的作用来说，$\widetilde{Q}(\mathrm{Exp}H)$ 是一个奇函数，亦即

$$\widetilde{Q}(\mathrm{Exp}\sigma H)) = \mathrm{sign}(\sigma)\cdot\widetilde{Q}(\mathrm{Exp}H),\sigma\in W,$$

其中 $\mathrm{sign}(\sigma)$ 就是 σ 作为 ζ 上正交变换的行列式的符号. 在 $\widetilde{Q}(\mathrm{Exp}H)$ 的展开式中有一个主导项，就是 $\mathrm{e}^{2\pi\mathrm{i}(\delta,H)}$，由上式可知，在 $\widetilde{Q}(\mathrm{Exp}H)$ 的展开式中就应包含所有的项 $\mathrm{sign}(\sigma)\cdot\mathrm{e}^{2\pi\mathrm{i}(\sigma\delta,H)}(\sigma\in W)$. 在它的展开式中不可能含有其他的项了，因此只能是

$$\widetilde{Q}(\mathrm{Exp}H) = Q(\mathrm{Exp}H).$$

6) 设 f 为定义在 G 上的任一中心函数. 在求积分 $\int_G f(g)\mathrm{d}g$ 时，我们先沿着 G- 轨道求积. 因为 f 在每个 G- 轨道 $G(t)$ 上都取等值，所以有

$$\int_G f(g)\mathrm{d}g = \int_{C_0} f(t)v(t)\mathrm{d}t$$

$$= \frac{1}{|W|}\int_T f(t)v(t)\mathrm{d}t = \frac{c}{|W|}\int_T f(t)\,|Q(t)|^2\mathrm{d}t,$$

其中 c 是一个待定常数，$|W|$ 是 W 的阶数（T 被分隔成 $|W|$ 个 Weyl 房），再将 $f(g)=1$ 的情形代入上式，就容易确定上述待定常数必为 1.

问题 7.8

1. 求证：环群的非平凡实不可约表示一定是二维的.

2. 设 G 是一个紧致连通 Lie 群，T 是它的一个极大子环群，$Z(G)$ 是 G 的中心. 求证：

(1) $G = \bigcup\limits_{q\in G} qTq^{-1}$.

(2) $Z(G) = \bigcap\limits_{q\in G} qTq^{-1}$.

3. 求证：设 D 是 Lie 代数 g 上的导子，则

$$\forall\, X,Y\in g, D^k[X,Y] = \sum_{i+j=k}\frac{k!}{i!\,j!}[D^iX,D^jY], k=0,1,2,\cdots$$

4. 设 φ_k 是在第一章 §4 所定义的 S^3 的 $(k+1)$ 维复不可约表示，求证

$$\Omega(\varphi_k) = \{k\theta,(k-2)\theta,\cdots,-(k-2)\theta,-k\theta\}.$$

5. 设 $W(S^3)$ 表示 S^3 的 Weyl 群，求证 $W(S^3)=\mathbf{Z}_2$.

6. 设 Λ_φ 是紧致连通 Lie 群 G 的复不可约表示 φ 的最高权，$\{\alpha_1,\cdots,\alpha_k\}$ 是 G 的根系 $\triangle(G)$ 在同一次序下的素根系. 求证：$\dfrac{2(\Lambda_\varphi,\alpha_i)}{(\alpha_i,\alpha_i)} = q_i$ 均为非负整数.

参考文献

1. 聂灵沼，丁石孙. 代数学引论. 北京：高等教育出版社，1988
2. 万哲先. 代数和编码(修订版). 北京：科学出版社，1980
3. 熊全淹. 近世代数. 武汉：武汉大学出版社，1984
4. 张端明，钟志成. 应用群论导引. 武汉：华中理工大学出版社，2001
5. 项武义等. 李群讲义. 北京：北京大学出版社，1992
6. Jacobson N. Basic Algebral. New York：W. H. Freeman and Company，1985
7. Kuczkowski J E，Garting J L. Abstract Algebra，a First Look. New York and Besel：Marcel Dekker，1977
8. Shafarevich I R. Basic Notions of Algebra，Encyclopaedia of Mathematical Sciences. Berlin：Springer-Verlag，1990
9. Nikulin V V，Shafarevich I R. Geometries and Groups. Beijing：Springer-Verlag，World Publishing Corporation，1989
10. Cox D，Little J，O'Shea D. Ideals，Varieties and Algorithms——An Introduction to Computational Algebraic Geometry and Commutative Algebra. New York：Springer-Verlag，1992